(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－23999
（P2002－23999A）
(43)公開日　平成14年１月25日(2002.1.25)

(51)Int.Cl.⁷		識別記号	FI			テーマコード(参考)
Ｇ０６Ｆ	7/552		Ｇ０６Ｆ	7/552	Ａ	５Ｊ１０４
	7/72			7/72		
Ｇ０９Ｃ	1/00	６５０	Ｇ０９Ｃ	1/00	６５０Ａ	

審査請求　有　　請求項の数33　ＯＬ　（全 22 頁）

(21)出願番号　特願2000－185582(P2000－185582)

(22)出願日　平成12年６月21日(2000.6.21)

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
INTERNATIONAL BUSINESS MASCHINES CORPORATION
アメリカ合衆国10504、ニューヨーク州　アーモンク　（番地なし）
(74)復代理人　100110607
弁理士　間山　進也　（外３名）

最終頁に続く

(54)【発明の名称】　乗算モジュール、乗法逆元演算回路、乗法逆元演算制御方式、該乗法逆元演算を用いる装置、暗号装置、誤り訂正復号器

(57)【要約】　（修正有）
【課題】　ガロア体GF(2ᵐ)（m≧1）上のｍビットデータを乗算するための乗算モジュールを提供する。
【解決手段】　第１の入力部からの第１のｍビットデータが入力される第１および第２のべき乗演算手段Ｕ１，Ｕ２と、第１のｍビットデータおよび第１のべき乗演算手段からの出力が入力される第１の乗算手段Ｕ３と、第２の入力部からの第２のｍビットデータおよび第２のべき乗演算手段Ｕ２からの出力が入力される第２の乗算手段Ｕ４と、第２の乗算手段の出力信号および第２のｍビットデータが入力される選択手段Ｕ５と、第１のべき乗演算手段には第１の制御信号Ｓ１が入力され、第２のべき乗乗算手段には第２の制御信号Ｓ２が入力され、選択手段には該選択手段の出力を制御するための第３の制御信号Ｓ０が入力され、前記第１の乗算手段が第１の出力信号を出力し、前記選択手段が第２の出力信号を出力する。

基本演算モジュール

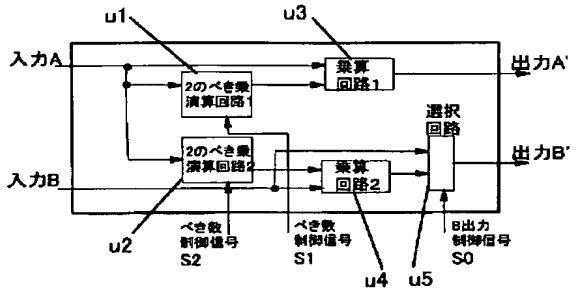


図4　回路の構成に用いる乗算デバイス

1

【特許請求の範囲】

【請求項１】　ガロア体GF(2m)（m≧1）上のｍビットデータを乗算するための第１の入力部と第２の入力部とを含む乗算モジュールであって、

前記第１の入力部からの第１のｍビットデータが入力される第１および第２のべき乗演算手段と、

前記第１のｍビットデータおよび前記第１のべき乗演算手段からの出力が入力される第１の乗算手段と、

前記第２の入力部からの第２のｍビットデータおよび前記第２のべき乗演算手段からの出力が入力される第２の乗算手段と、

前記第２の乗算手段の出力信号および前記第２のｍビットデータが入力される選択手段と、

前記第１のべき乗演算手段と、前記第２のべき乗演算手段と、前記選択手段とにそれぞれ制御信号を出力する制御手段とを含んで構成され、

前記第１のべき乗演算手段には第１の制御信号が入力され、前記第２のべき乗乗算手段には第２の制御信号が入力され、前記選択手段には該選択手段の出力を制御するための第３の制御信号が入力され、前記第１の乗算手段が第１の出力信号を出力し、前記選択手段が第２の出力信号を出力する、乗算モジュール。

【請求項２】　請求項１の乗算モジュールと、

第１の初期値が設定でき前記乗算モジュールの第１の出力信号が入力される、第１のレジスタ手段と、

第２の初期値が設定でき前記乗算モジュールの第２の出力信号が入力される、第２のレジスタ手段とを含み、

前記第１のレジスタ手段の出力が前記乗算モジュールの第１の入力部に接続され、前記第２のレジスタ手段の出力が前記乗算モジュールの第２の入力部に接続されており、

前記第２のレジスタ手段が、前記第１、第２、第３の制御信号に応じて前記第１の初期値の乗法逆元を与える、乗法逆元演算回路。

【請求項３】　前記第１の初期値と前記第２の初期値とをレジスタ手段へ入力し、前記制御手段は、サイクル数が所定の数ｋ（ｋは、自然数）となった場合に第１のべき乗演算手段にｒ＝2^{k-1}、ｓ＝２ｒとしてｓ乗を計算させる第１の制御信号と、第２のべき乗演算手段にｒ＝｛（ｍ－１）ｍｏｄ（2^{k-1}）｝＋１、ｓ＝２ｒとしてｓ乗を計算させる第２の制御信号とを入力し、前記乗算モジュールの選択手段には、（ｍ－１）の２進表現でのビットｋ－１が１の場合には前記第２のレジスタ手段の入力に前記第２の乗算手段の出力を入力し、（ｍ－１）の２進表現でのビットｋ－１が１でない場合には前記第２のレジスタ手段の入力に前記第２のレジスタ手段の出力を与える第３の制御信号を入力する、請求項２に記載の乗法逆元演算回路。

【請求項４】　請求項１の乗算モジュール２個と、第１の初期値が設定できる第１のレジスタ手段と、第２の初期値が設定できる第２のレジスタ手段とを含み、前記乗算モジュールのそれぞれ第１の出力を他の前記第１の入力部に接続し、前記乗算モジュールのそれぞれ第２の出力を他の前記第２の入力部に接続し、

前記乗算モジュール群の結合によって得られた回路に対し、前記乗算モジュールの第１の入力部に前記第１のレジスタ手段の出力が接続され、前記乗算モジュールの第２の入力部に前記第２のレジスタ手段の出力が接続され、前記乗算モジュールの第１の出力部に前記第１のレジスタ手段の入力が接続され、前記乗算モジュールの第２の出力部に前記第２のレジスタ手段の入力が接続された乗法逆元演算回路。

【請求項５】　３個以上の請求項１の乗算モジュールと、第１の初期値が設定できる第１のレジスタ手段と、第２の初期値が設定できる第２のレジスタ手段とを含み、前記乗算モジュールのそれぞれ第１の出力を他の前記第１の入力部に接続し、前記乗算モジュールのそれぞれ第２の出力を他の前記第２の入力部に接続し、

前記乗算モジュール群の結合によって得られた回路に対し、前記乗算モジュールの第１の入力部に前記第１のレジスタ手段の出力が接続され、前記乗算モジュールの第２の入力部に前記第２のレジスタ手段の出力が接続され、前記乗算モジュールの第１の出力部に前記第１のレジスタ手段の入力が接続され、前記乗算モジュールの第２の出力部に前記第２のレジスタ手段の入力が接続された乗法逆元演算回路。

【請求項６】　前記乗算モジュールの数ｎ（ｎは、自然数）は、$[\log_2(m-1)+1]$以下とされる、請求項４または５に記載の乗法逆元演算回路。

【請求項７】　制御手段により、ｉ段目（ｎ≧ｉ≧１）の乗算モジュールに対して、サイクル数が所定の数ｑ（ｑは自然数）となった場合に、ｐ＝｛ｎ（ｑ－１）＋ｉ｝として、第１のべき乗演算手段にｒ＝2^{p-1}、ｓ＝２ｒとしてｓ乗を計算させる第１の制御信号と、第２のべき乗演算手段にｒ＝｛（ｍ－１）ｍｏｄ（2^{p-1}）｝＋１、ｓ＝２ｒとしてｓ乗を計算させる第２の制御信号とを入力し、前記ｉ段目の乗算モジュールの選択手段には、（ｍ－１）の２進表現でのビットｐ－１が１の場合には前記ｉ段目の乗算モジュールの第２の出力に前記第２の乗算手段の出力を与え、（ｍ－１）の２進表現でのビットｐ－１が１でない場合には前記ｉ段目のモジュールの第２の出力に、前記ｉ段目の乗算モジュールへの第２の入力部からのｍビットデータを与える第３の制御信号を入力する、請求項４、５または６に記載の乗法逆元演算回路。

【請求項８】　$[\log_2(m-1)+1]$個の請求項１の乗算モジュールと、

それぞれの前記乗算モジュールを制御するための第１の制御信号群と、第２の制御信号群と、第３の制御信号群とを与える制御手段とを含み、

前記乗算モジュールのそれぞれ第１の出力が次の前記乗算モジュールの第１の入力部に接続され、前記乗算モジュールのそれぞれ第２の出力が次の前記乗算モジュールの前記第２の入力部に接続されており、

前記制御手段は、所定段目ｋ（ｋは、自然数）の乗算モジュールに対して、ｒ＝２$^{k-1}$、ｓ＝２ｒとしてｓ乗を計算させる第１の制御信号を第１のべき乗演算手段に与え、ｒ＝｛（ｍ－１）ｍｏｄ（２$^{k-1}$）｝＋１、ｓ＝２ｒとしてｓ乗を計算させる第２の制御信号を第２のべき乗演算手段に与え、ｍ－１の２進表現におけるビットｋ－１が１の場合に選択手段の出力として第２の乗算手段の出力を与え、ｍ－１の２進表現におけるビットｋ－１が１ではない場合には選択手段の出力として第２の入力部から入力されるｍビットデータを与える、乗法逆元演算回路。

【請求項９】　前記乗算モジュールに接続される対となったレジスタ手段を含む、請求項８に記載の乗法逆元演算回路。

【請求項１０】　ガロア体GF(2^m)（ｍ≧１）上のｍビットデータを乗算するための第１の入力部と第２の入力部とを含む乗算モジュールの制御方式であって、

第１および第２のべき乗演算手段に前記第１の入力部からの第１のｍビットデータを入力する段階と、

第１の乗算手段に前記第１のｍビットデータおよび前記第１のべき乗演算手段からの出力を入力する段階と、

第２の乗算手段に前記第２の入力部からの第２のｍビットデータおよび前記第２のべき乗演算手段からの出力を入力する段階と、

選択手段に前記第２の乗算手段の出力信号および前記第２のｍビットデータを入力する段階と、

制御回路から前記第１の乗算手段と、前記第２の乗算手段と、前記選択手段とにそれぞれ制御信号を出力する段階とを含み、

前記第１のべき乗演算手段に第１の制御信号を入力し、

前記第２のべき乗演算手段に第２の制御信号を入力し、

前記選択手段に該選択手段の出力を制御するための第３の制御信号を入力し、前記第１の乗算手段に第１の出力信号を出力させ、前記選択手段に第２の出力信号を出力させる、乗算モジュールの制御方式。

【請求項１１】　請求項１の乗算モジュールを与える段階と、

第１の初期値が設定でき前記乗算モジュールの第１の出力信号が入力される、第１のレジスタ手段を与える段階と、

第２の初期値が設定でき前記乗算モジュールの第２の出力信号が入力される、第２のレジスタ手段を与える段階とを含み、前記第１のレジスタ手段の出力が前記乗算モジュールの第１の入力部に接続され、前記第２のレジスタ手段の出力が前記乗算モジュールの第２の入力部に接続されており、

さらに、前記第２のレジスタ手段が、前記第１、第２、第３の制御信号に応じて前記第１の初期値の乗法逆元を与える段階とを含む、乗法逆元演算回路の制御方式。

【請求項１２】　前記第１の初期値と前記第２の初期値とを入力する段階と、サイクル数が所定の数ｋ（ｋは、自然数）となった場合に第１のべき乗演算手段にｒ＝２$^{k-1}$、ｓ＝２ｒとしてｓ乗を計算させる第１の制御信号と、第２のべき乗演算手段にｒ＝｛（ｍ－１）ｍｏｄ（２$^{k-1}$）｝＋１、ｓ＝２ｒとしてｓ乗を計算させる第２の制御信号とを入力し、前記乗算モジュールの選択手段には、（ｍ－１）の２進表現でのビットｋ－１が１の場合には前記第２のレジスタ手段の入力に前記第２の乗算手段の出力を入力し、（ｍ－１）の２進表現でのビットｋ－１が１でない場合には前記第２のレジスタ手段の入力に前記第２のレジスタ手段の出力を入力するための第３の制御信号を入力する段階を含む、請求項１１に記載の乗法逆元演算回路の制御方式。

【請求項１３】　請求項１の乗算モジュール２個と、第１の初期値が設定できる第１のレジスタ手段と、第２の初期値が設定できる第２のレジスタ手段とを含み、前記乗算モジュールのそれぞれ第１の出力を他の前記第１の入力部に接続し、前記乗算モジュールのそれぞれ第２の出力を他の前記第２の入力部に接続した乗法逆元演算回路の制御方式であって、前記乗算モジュールの第１の出力部に前記第１のレジスタ手段の入力が接続され、前記乗算モジュールの第２の出力部に前記第２のレジスタ手段の入力が接続され、

前記乗算モジュール群の結合によって得られた回路に対し、前記乗算モジュールの第１の入力部に前記第１のレジスタ手段の出力を接続する段階と、前記乗算モジュールの第２の入力部に前記第２のレジスタ手段の出力を接続する段階と、を含む、乗法逆元演算回路の制御方式。

【請求項１４】　３個以上の請求項１の乗算モジュール２個と、第１の初期値が設定できる第１のレジスタ手段と、第２の初期値が設定できる第２のレジスタ手段とを含み、前記乗算モジュールのそれぞれ第１の出力を他の前記第１の入力部に接続し、前記乗算モジュールのそれぞれ第２の出力を他の前記第２の入力部に接続した乗法逆元演算回路の制御方式であって、前記乗算モジュールの第１の出力部に前記第１のレジスタ手段の入力が接続され、前記乗算モジュールの第２の出力部に前記第２のレジスタ手段の入力が接続され、

前記乗算モジュール群の結合によって得られた回路に対し、前記乗算モジュールの第１の入力部に前記第１のレジスタ手段の出力を接続する段階と、前記乗算モジュールの第２の入力部に前記第２のレジスタ手段の出力を接続する段階とを含む、乗法逆元演算回路の制御方式。

【請求項１５】　前記乗算モジュールの数ｎ（ｎは、自然数）は、$[\log_2(m-1)+1]$以下とされる、請求項１３または１４に記載の乗法逆元演算回路の制御方式。

5

【請求項１６】　ｉ段目（ｎ≧ｉ≧１）の乗算モジュールに対して、サイクル数が所定の数ｑ（ｑは自然数）となった場合に、ｐ＝｛ｎ（ｑ－１）＋ｉ｝として、第１のべき乗演算手段にｒ＝2^{p-1}、ｓ＝２ｒとしてｓ乗を計算させる第１の制御信号と、第２のべき乗演算手段にｒ＝｛（ｍ－１）ｍｏｄ（2^{p-1}）｝＋１、ｓ＝２ｒとしてｓ乗を計算させる第２の制御信号とを入力し、前記乗算モジュールの選択手段には、（ｍ－１）の２進表現でのビットｐ－１が１の場合には前記ｉ段目の乗算モジュールの第２の出力に前記第２の乗算手段の出力を与え、（ｍ－１）の２進表現でのビットｐ－１が１でない場合には前記ｉ段目の乗算モジュールの第２の出力に、前記ｉ段目の乗算モジュールの第２の入力部からのｍビットデータを与える第３の制御信号を入力する、請求項１３、１４または１６に記載の乗法逆元演算回路の制御方式。

【請求項１７】　$[\log_2(m-1)+1]$個の請求項１の乗算モジュールを与える段階と、

それぞれの前記乗算モジュールを制御するための第１の制御信号群と、第２の制御信号群と、第３の制御信号群とを与える段階とを含み、前記乗算モジュールのそれぞれ前記第１の出力が次の前記第１の入力部に接続され、前記乗算モジュールのそれぞれ前記第２の出力が次の前記第２の入力部に接続されており、

所定段目ｋ（ｋは、自然数）の乗算モジュールに対して、ｒ＝2^{k-1}、ｓ＝２ｒとしてｓ乗を計算させる第１の制御信号を第１のべき乗演算手段に与え、ｒ＝｛（ｍ－１）ｍｏｄ（2^{k-1}）｝＋１、ｓ＝２ｒとしてｓ乗を計算させる第２の制御信号を第２のべき乗演算手段に与え、ｍ－１の２進表現におけるビットｋ－１が１の場合に選択手段の出力として第２の乗算手段の出力を与え、ｍ－１の２進表現におけるビットｋ－１が１ではない場合には選択手段の出力として第２の入力部から入力されるｍビットデータを与える段階を含む、乗法逆元演算回路の制御方式。

【請求項１８】　前記乗算モジュールからの出力を対となったレジスタ手段に入力する段階を含む、請求項１２、１３、または１４に記載の乗法逆元演算回路。

【請求項１９】　ガロア体GF(2^m)（ｍ≧１）上のｍビットデータを乗算するための第１の入力部と第２の入力部とを含む乗算モジュールを用いる装置であって、該乗算モジュールは、

前記第１の入力部からの第１のｍビットデータが入力される第１および第２のべき乗演算手段と、

前記第１のｍビットデータおよび前記第１のべき乗演算手段からの出力が入力される第１の乗算手段と、

前記第２の入力部からの第２のｍビットデータおよび前記第２のべき乗演算手段からの出力が入力される第２の乗算手段と、

前記第２の乗算手段の出力信号および前記第２のｍビットデータが入力される選択手段と、

6

前記第１のべき乗演算手段と、前記第２のべき乗演算手段と、前記選択手段とにそれぞれ制御信号を出力する制御回路とを含んで構成され、

前記第１のべき乗演算手段には第１の制御信号が入力され、前記第２のべき乗乗算手段には第２の制御信号が入力され、前記選択手段には該選択手段の出力を制御するための第３の制御信号が入力され、前記第１の乗算手段が第１の出力信号を出力し、前記選択手段が第２の出力信号を出力する装置。

【請求項２０】　請求項１の乗算モジュールと、

第１の初期値が設定でき前記乗算モジュールの第１の出力信号が入力される、第１のレジスタ手段と、

第２の初期値が設定でき前記乗算モジュールの第２の出力信号が入力される、第２のレジスタ手段とを含み、

前記第１のレジスタ手段の出力が前記乗算モジュールの第１の入力部に接続され、前記第２のレジスタ手段の出力が前記乗算モジュールの第２の入力部に接続されており、

前記第２のレジスタ手段が、前記第１、第２、第３の制御信号に応じて前記第１の初期値の乗法逆元を与える、乗法逆元演算回路を含む装置。

【請求項２１】　前記第１の初期値と前記第２の初期値とを入力し、サイクル数が所定の数ｋ（ｋは、自然数）となった場合に第１のべき乗演算手段にｒ＝2^{k-1}、ｓ＝２ｒとしてｓ乗を計算させる第１の制御信号と、第２のべき乗演算手段にｒ＝｛（ｍ－１）ｍｏｄ（2^{k-1}）｝＋１、ｓ＝２ｒとしてｓ乗を計算させる第２の制御信号とを入力し、前記乗算モジュールの選択手段には、（ｍ－１）の２進表現でのビットｋ－１が１の場合には前記第２のレジスタ手段の入力に前記第２の乗算手段の出力を入力し、（ｍ－１）の２進表現でのビットｋ－１が１でない場合には前記第２のレジスタ手段の入力に前記第２のレジスタ手段の出力を入力するための第３の制御信号を入力する、乗法逆元演算回路を含む請求項２０に記載の装置。

【請求項２２】　請求項１の乗算モジュール２個と、第１の初期値が設定できる第１のレジスタ手段と、第２の初期値が設定できる第２のレジスタ手段とを含み、前記乗算モジュールのそれぞれ第１の出力を他の前記第１の入力部に接続し、前記乗算モジュールのそれぞれ第２の出力を他の前記第２の入力部に接続し、

前記乗算モジュール群の結合によって得られた回路に対し、その第１の入力部に前記第１のレジスタ手段の出力が接続され、前記乗算モジュールの第２の入力部に前記第２のレジスタ手段の出力が接続され、前記乗算モジュールの第１の出力部に前記第１のレジスタ手段の入力が接続され、前記乗算モジュールの第２の出力部に前記第２のレジスタ手段の入力が接続された乗法逆元演算回路を含む、装置。

7

【請求項２３】　３個以上の請求項１の乗算モジュールと、第１の初期値が設定できる第１のレジスタ手段と、第２の初期値が設定できる第２のレジスタ手段とを含み、前記乗算モジュールのそれぞれ第１の出力を他の前記第１の入力部に接続し、前記乗算モジュールのそれぞれ第２の出力を他の前記第２の入力部に接続し、
前記乗算モジュール群の結合によって得られた回路に対し、その第１の入力部に前記第１のレジスタ手段の出力が接続され、前記乗算モジュールの第２の入力部に前記第２のレジスタ手段の出力が接続され、前記乗算モジュールの第１の出力部に前記第１のレジスタ手段の入力が接続され、前記乗算モジュールの第２の出力部に前記第２のレジスタ手段の入力が接続された乗法逆元演算回路を含む、装置。

【請求項２４】　前記乗算モジュールの数ｎ（ｎは、自然数）は、$[\log_2(m-1)+1]$以下とされる乗法逆元演算回路を含む請求項２２または２３に記載の装置。

【請求項２５】　前記制御手段により、ｉ段目（ｎ≧ｉ≧１）の乗算モジュールに対して、サイクル数が所定の数ｑ（ｑは自然数）となった場合に、ｐ＝｛ｎ（ｑ－１）＋ｉ｝として、第１のべき乗演算手段にｒ＝2^{p-1}、ｓ＝２ｒとしてｓ乗を計算させる第１の制御信号と、第２のべき乗演算手段にｒ＝｛（ｍ－１）ｍｏｄ（2^{p-1}）｝＋１、ｓ＝２ｒとしてｓ乗を計算する第２の制御信号とを入力し、前記ｉ番目の乗算モジュールの選択手段には、（ｍ－１）の２進表現でのビットｐ－１が１の場合には前記ｉ番目の乗算モジュールの第２の出力に前記第２の乗算手段の出力を与え、（ｍ－１）の２進表現でのビットｐ－１が１でない場合には前記ｉ番目の乗算モジュールの第２の出力を、前記ｉ段目の乗算モジュールの第２の入力部からのｍビットデータとする第３の制御信号を入力する乗法逆元演算回路を含む、請求項２２、２３または２４に記載の装置。

【請求項２６】　$[\log_2(m-1)+1]$個の請求項１の乗算モジュールと、
それぞれの前記乗算モジュールを制御するための第１の制御信号群と、第２の制御信号群と、第３の制御信号群とを与える制御手段とを含み、
前記乗算モジュールのそれぞれ第１の出力が他の前記乗算モジュールの第１の入力部に接続され、前記乗算モジュールのそれぞれ第２の出力が他の前記乗算モジュールの第２の入力部に接続されており、
前記制御手段は、所定段目ｋ（ｋは、自然数）の乗算モジュールに対して、ｒ＝2^{k-1}、ｓ＝２ｒとしてｓ乗を計算させる第１の制御信号を第１のべき乗演算手段に与え、ｒ＝｛（ｍ－１）ｍｏｄ（2^{k-1}）｝＋１、ｓ＝２ｒとしてｓ乗を計算させる第２の制御信号を第２のべき乗演算手段に与え、ｍ－１の２進表現におけるビットｋ－１が１の場合に選択手段の出力として第２の乗算手段の出力を与え、ｍ－１の２進表現におけるビットｋ－１が１ではない場合には選択手段の出力として前記第２の入力部から入力されるｍビットデータを与える乗法逆元演算回路を含む装置。

8

【請求項２７】　前記乗算モジュールに接続される対となったレジスタ手段を含む、請求項２２、２３または２４に記載の乗法逆元演算回路を含む装置。

【請求項２８】　ガロア体GF(2^m)（ｍ≧１）上のｍビットデータを乗算するため、第１の入力部からｍビットデータおよびべき乗演算手段からの出力を乗算手段に入力する段階と、第２の入力部からのｍビットデータおよび前記べき乗演算手段からの出力を乗算手段に入力する段階とを含む乗法逆元演算回路の制御方式であって、
ｐ＝｛ｎ（ｑ－１）＋ｉ｝として、第１のべき乗演算手段にｒ＝2^{p-1}、ｓ＝２ｒとしてｓ乗を計算させる第１の制御信号と、第２のべき乗演算手段にｒ＝｛（ｍ－１）ｍｏｄ（2^{p-1}）｝＋１、ｓ＝２ｒとしてｓ乗を計算する第２の制御信号とを入力する段階と、
ｍ－１の２進表現におけるビットｋ－１（ｋは、自然数）が１の場合に選択手段の出力として第２の乗算手段の出力を与え、ｍ－１の２進表現におけるビットｋ－１が１ではない場合には選択手段の出力として前記第２の入力部から入力されるｍビットデータを与える段階とを含む、乗法逆元演算回路の制御方式。

【請求項２９】　ガロア体GF(2^m)（ｍ≧１）上のｍビットデータを乗算するため、第１の入力部からｍビットデータおよびべき乗演算手段からの出力を乗算手段に入力する段階と、第２の入力部からのｍビットデータおよび前記べき乗演算手段からの出力を乗算手段に入力する段階とを含む乗算方法を実行させるためのソースコードが記録されたコンピュータ可読な記録媒体であって、該記録媒体は、ｐ＝｛ｎ（ｑ－１）＋ｉ｝として、第１のべき乗演算手段にｒ＝2^{p-1}、ｓ＝２ｒとしてｓ乗を計算させる第１の制御信号と、第２のべき乗演算手段にｒ＝｛（ｍ－１）ｍｏｄ（2^{p-1}）｝＋１、ｓ＝２ｒとしてｓ乗を計算する第２の制御信号とを入力し、
ｍ－１の２進表現におけるビットｋ－１（ｋは、自然数）が１の場合に選択手段の出力として第２の乗算手段の出力を与え、ｍ－１の２進表現におけるビットｋ－１が１ではない場合には選択手段の出力として前記第２の入力部から入力されるｍビットデータを与える、記録媒体。

【請求項３０】　ガロア体GF(2^m)（ｍ≧１）上のｍビットデータを乗算するため、第１の入力部からｍビットデータおよびべき乗演算手段からの出力を乗算手段に入力する段階と、第２の入力部からのｍビットデータおよび前記べき乗演算手段からの出力を乗算手段に入力する段階とを含む乗算方法を実行させるためのソースコードが記録されたコンピュータ可読な伝送媒体であって、該伝送媒体は、
ｐ＝｛ｎ（ｑ－１）＋ｉ｝として、第１のべき乗演算手

9

段にｒ＝2^{p-1}、ｓ＝２ｒとしてｓ乗を計算させる第１の制御信号と、第２のべき乗演算手段にｒ＝｛（ｍ－１）ｍｏｄ（2^{p-1}）｝＋１、ｓ＝２ｒとしてｓ乗を計算する第２の制御信号とを入力し、

ｍ－１の２進表現におけるビットｋ－１（ｋは、自然数）が１の場合に選択手段の出力として第２の乗算手段の出力を与え、ｍ－１の２進表現におけるビットｋ－１が１ではない場合には選択手段の出力として前記第２の入力部から入力されるｍビットデータを与える、伝送媒体。

【請求項３１】　ガロア体GF(2ᵐ)（ｍ≧1）上のｍビットデータを乗算するため、第１の入力部からのｍビットデータおよびべき乗演算手段からの出力が入力される乗算手段と、第２の入力部からのｍビットデータおよび前記べき乗演算手段からの出力が入力される乗算手段とを含む暗号装置であって、

ｐ＝｛ｎ（ｑ－１）＋ｉ｝として、第１のべき乗演算手段にｒ＝2^{p-1}、ｓ＝２ｒとしてｓ乗を計算させる第１の制御信号と、第２のべき乗演算手段にｒ＝｛（ｍ－１）ｍｏｄ（2^{p-1}）｝＋１、ｓ＝２ｒとしてｓ乗を計算させる第２の制御信号とを入力するための手段と、

ｍ－１の２進表現におけるビットｋ－１（ｋは、自然数）が１の場合に選択手段の出力として第２の乗算手段の出力を与え、ｍ－１の２進表現におけるビットｋ－１が１ではない場合には選択手段の出力として前記第２の入力部から入力されるｍビットデータを与えるための手段と、を含む暗号装置。

【請求項３２】　ガロア体GF(2ᵐ)（ｍ≧1）上のｍビットデータを乗算するため、第１の入力部からのｍビットデータおよびべき乗演算手段からの出力が入力される乗算手段と、第２の入力部からのｍビットデータおよび前記べき乗演算手段からの出力が入力される乗算手段とを含む誤り訂正復号器であって、

ｐ＝｛ｎ（ｑ－１）＋ｉ｝として、第１のべき乗演算手段にｒ＝2^{p-1}、ｓ＝２ｒとしてｓ乗を計算させる第１の制御信号と、第２のべき乗演算手段にｒ＝｛（ｍ－１）ｍｏｄ（2^{p-1}）｝＋１、ｓ＝２ｒとしてｓ乗を計算する第２の制御信号とを入力するための手段と、

ｍ－１の２進表現におけるビットｋ－１（ｋは、自然数）が１の場合に選択手段の出力として第２の乗算手段の出力を与え、ｍ－１の２進表現におけるビットｋ－１が１ではない場合には選択手段の出力として前記第２の入力部から入力されるｍビットデータを与えるための手段と、を含む誤り訂正復号器。

【請求項３３】　ガロア体GF(2ᵐ)（ｍ≧1）上のｍビットデータを乗算するため、第１の入力部からのｍビットデータおよびべき乗演算手段からの出力が入力される乗算手段と、第２の入力部からのｍビットデータおよび前記べき乗演算手段からの出力が入力される乗算手段とを含む装置であって、

10

ｐ＝｛ｎ（ｑ－１）＋ｉ｝として、第１のべき乗演算手段にｒ＝2^{p-1}、ｓ＝２ｒとしてｓ乗を計算させる第１の制御信号と、第２のべき乗演算手段にｒ＝｛（ｍ－１）ｍｏｄ（2^{p-1}）｝＋１、ｓ＝２ｒとしてｓ乗を計算する第２の制御信号とを入力するための手段と、

ｍ－１の２進表現におけるビットｋ－１（ｋは、自然数）が１の場合に選択手段の出力として第２の乗算手段の出力を与え、ｍ－１の２進表現におけるビットｋ－１が１ではない場合には選択手段の出力として前記第２の入力部から入力されるｍビットデータを与えるための手段と、を含む装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、乗算モジュール、乗法逆元演算回路、乗法逆元演算回路の制御方式、および装置に関し、より詳細には、ガロア拡大体ＧＦ（2^m）（ｍは任意の自然数）の乗法逆元演算を、低レイテンシかつ小規模な回路によって実現することを可能とする乗算モジュール、乗法逆元演算回路、乗法逆元演算回路の制御方式、装置、暗号装置および誤り訂正復号器に関する。

【０００２】

【従来の技術】まず、本発明も含めて、ハードウェア向けの逆数演算アルゴリズムの評価ポイントは次のとおり：

（１）乗算器の個数

（２）レジスタの個数

（３）レイテンシ（順序回路の場合はクロック数＊クロック周波数）。これは行う乗算の回数に強く依存する。

（４）順序回路の場合、最大動作周波数。当然ながら、同じクロック数で計算ができるなら、最大動作周波数が高い回路がよい。同じ最大動作周波数なら、少ないクロック数で計算ができる回路がよい。

上記の各ポイントについて従来手法や本発明がどうであるかは、後に比較として述べるので、以下では従来手法の概要についてまずまとめる。

【0-0-0３】方法１：Fermat's little theōrēm

文献[1]や[4]などに示されているとおり、

【０００４】

【数１】

$$x^{-1} = x^{2^m-2} = x^{2^1} x^{2^2} \cdots x^{2^{m-1}}$$

の公式（Fermatの小定理）を用いて乗法逆元を計算できる。この式のとおりに計算を進めると、ｍ－２回の乗算が必要である。

【０００５】この公式の計算を順序回路として作る場合には、図１に示した計算過程に基づいて、１個の乗算回路と１個の２乗回路を持ち、（ｘ２）のｉ乗を求めながら（ｍ－２）回のループで計算するアルゴリズムがよく使われている。レイテンシ（サイクル数）は（ｍ－２）

11

となる。

【０００６】組み合わせ回路で実現する場合は、図２のように木構造を作れば、Ｍを乗算回路のレイテンシとして

【０００７】

【数２】

$$M\{[\log_2(m-2)+1]\}$$

のレイテンシとなる（一般に、べき条演算のレイテンシはごく小さいので無視する）。

【０００８】方法２：伊東･辻井のアルゴリズムと、その類似手法

文献[2]に、これまで知られている限りもっとも乗算回数が少なくて済むアルゴリズム（伊東･辻井のアルゴリズム）が示されている。図３にｍ＝１６における計算過程の例を示す。また、このアルゴリズムより以前に伊東らが文献[3]で提案した別アルゴリズムに、

【０００９】

【数３】

$$2^k-1=2\ (2^{k/2}-1)\ (2^{k/2}+1)$$

等の関係を用いてべき数２ｍ－２を再帰的に２分解し、実計算はその逆の手順でボトムアップに乗算およびべき乗演算を進める、という方法もある。いずれのアルゴリズムでも、順序回路にしたときサイクル数は、

【００１０】

【数４】

$$[\log_2(m-1)]+Hw(m-1)-1$$

であり、組み合わせ回路にしたときレイテンシは、Ｍを乗算回路のレイテンシとして

【００１１】

【数５】

$$M\{[\log_2(m-1)]+Hw(m-1)-1\}$$

となる（べき乗演算のレイテンシは、ごく小さいので無視した）。

【００１２】いずれのアルゴリズムでも、方法１と異なり、各乗算を逐次的に進めないと正しい計算結果が得られないという問題点がある。

【００１３】方法３：乗算と部分体上での乗法逆元演算の組み合わせによる方法

文献[4]，[2]などに、ＧＦ（２ｍ）においてｍ＝ｋｑ（ｍが合成数）であるとき、ＧＦ（２ｍ）の乗法逆元演算をＧＦ（２ｍ）の乗算とＧＦ（２ｋ）（ないしＧＦ（２ｑ））の乗法逆元演算に帰着する方法が示されている。これにより、うまく原始多項式や表現基底を選定すれば、かなり回路規模が縮小され、回路速度も速くなる場合が存在する。

【００１４】しかし、この方法は限られた特定の場合にしか使えないという問題がある。たとえばｍが素数であればまったく使えないし、ターゲットの体ＧＦ（２ｍ）の原始多項式によっては、回路規模や速度の向上が得られないこともある。

12

【００１５】方法４：ユークリッド互除法

文献[5]等では、多項式上でユークリッド互除法を用いて乗法逆元を計算する方法が示されている。これは、入力多項式（乗法逆元を求めたい多項式）をＡ、原始多項式をＦとしたとき、ユークリッド互除法でＢＡ＋ＦＭ＝１を満たすＢ，Ｍを求めると、ガロア体上ではＢがＡの乗法逆元となるという性質を利用したものである。この方法は、一般にレイテンシがＯ（ｍ）となるという問題点がある。

【００１６】代表的な文献：

[1] S. B. Wicker and V. K. Bhargava (eds.), Reed-Solomon Codes and Their Applications, IEEE Press, 1994.

[2] T. Itoh and S. Tsujii, "A Fast Algorithm for Computing MultiplicativeInverses inGF(2m) Using Normal Bases," Information and Computation, vol. 78, no. 3, pp. 171-177, 1988.

[3] T. Itoh, O. Teechai and S. Tsujii, "A fast algorithm for computing multiplicative inverses in GF(2m) using normal bases, J. Society for Electronic Communications (Japan), 44, 31-36, 1986.

[4] J. Guajardo and C. Paar, "Efficient Algorithms for Elliptic Curve Cryptosystems," proc. of 17th Annual Intl. Cryptology Conf. (CRYPTO'97), LNCS1294, pp. 342-356, 1997.

[5] H. Brunner, A. Curiger and M. Hofstetter, "On computing multiplicativeinverses in GF(2m)", IEEE Trans. Computers, vol. 42, pp. 1010-1015, 1993.

【００１７】

【発明が解決しようとする課題】伊東のアルゴリズムでは、乗算回数は少ないが、回路のレイテンシが大きくなるという問題がある．逆にＦｅｒｍａｔでは，組み合わせ回路にしたとき、レイテンシは小さいが回路規模が大きくなり、順序回路にしたとき、レイテンシが大きくなる、という問題がある。

【００１８】本発明では両方の手法の良い部分をとり、順序回路、組み合わせ回路のいずれの場合についても、小規模、低レイテンシを、一度に達成する。本発明は、通常の回路設計で良くあるようなスピードとエリアのトレードオフを図る話ではなく、それらを両方改善するものである。

【００１９】本発明は、任意のｍを対象として、基本モジュールを組み合わせた形で、低いレイテンシ（順序回路の場合は少ない処理クロック数、組み合わせ回路の場合は少ディレイ）を乗算回数を増やすことなく達成するものである。既存の方法では、いずれもレイテンシを減らすこと自体が困難か、レイテンシを減らそうとすると回路規模がたいへん大きくなるという問題があった。具体的には、以下の通りである。

13

【００２０】（１）Fermatの定理をそのまま計算する方法では、組み合わせ回路にすればレイテンシは、

【００２１】

【数６】

$$M\{[\log_2(m-2)]+1\}$$

にまで改善できるが、乗算回路がｍ－２個必要となる。

【００２２】（２）伊東・辻井の方法、およびその類似手法では、全体として行われる乗算の回数は、

【００２３】

【数７】

$$M([\log_2(m-1)]+Hw(m-1)-1)$$

となり、Fermatよりも悪い。

【００２６】（４）部分体上の除算へ帰着する方法は、限られたｍや原始多項式でしか使えない。なお、この方法は本発明と対立する手法ではなく、本手法と組み合わせて併用すれば、さらに回路性能を改善できる。

【００２７】（５）ユークリッド互除法による方法は、Ｏ（ｍ）のレイテンシがかかり、その改善は簡単でないという問題点がある。

【００２８】本手法は、乗算の全回数が伊東・辻井とまったく同じ（Ｆｅｒｍａｔより少ない）にも関わらず、レイテンシが最高で伊東・辻井の約半分（Ｆｅｒｍａｔと同じ）に改善できる。

【００２９】

【課題を解決するための手段】乗法逆元計算は乗算やべき乗演算を利用して行うが、計算の進め方によって得られる回路の性能が変わる。本発明は、基本モジュールを組み合わせた形で、低いレイテンシ（順序回路の場合は少ない処理クロック数、組み合わせ回路の場合は少ディレイ）を乗算回数を増やすことなく達成するものである。

【００３０】すなわち、本発明の上記課題は、本発明の乗算モジュール、乗法逆元演算回路、該乗法逆元演算回路の制御方式、装置、暗号装置および誤り訂正復号器を提供することにより解決される。

【００３１】すなわち、本発明の請求項１の発明によれば、ガロア体GF(2ᵐ)（ｍ≧1）上のｍビットデータを乗算するための第１の入力部と第２の入力部とを含む乗算モジュールであって、前記第１の入力部からの第１のｍビットデータが入力される第１および第２のべき乗演算手段と、前記第１のｍビットデータおよび前記第１のべき乗演算手段からの出力が入力される第１の乗算手段と、前記第２の入力部からの第２のｍビットデータおよび前記第２のべき乗演算手段からの出力が入力される第２の乗算手段と、前記第２の乗算手段の出力信号および前記第２のｍビットデータが入力される選択手段と、前記第１のべき乗演算手段と、前記第２のべき乗演算手段と、前記選択手段とにそれぞれ制御信号を出力する制御手段

14

$$[\log_2(m-1)]+Hw(m-1)-1$$

個で済むが、レイテンシを改善することが困難である。

レイテンシは、順序回路で、

【００２４】

【数８】

$$[\log_2(m-1)]+Hw(m-1)-1$$

サイクル、組み合わせ回路では、

【００２５】

【数９】

とを含んで構成され、前記第１のべき乗演算手段には第１の制御信号が入力され、前記第２のべき乗乗算手段には第２の制御信号が入力され、前記選択手段には該選択手段の出力を制御するための第３の制御信号が入力され、前記第１の乗算手段が第１の出力信号を出力し、前記選択手段が第２の出力信号を出力する、乗算モジュールが提供される。

【００３２】本発明の請求項２の発明によれば、請求項１の乗算モジュールと、第１の初期値が設定でき前記乗算モジュールの第１の出力信号が入力される、第１のレジスタ手段と、第２の初期値が設定でき前記乗算モジュールの第２の出力信号が入力される、第２のレジスタ手段とを含み、前記第１のレジスタ手段の出力が前記乗算モジュールの第１の入力部に接続され、前記第２のレジスタ手段の出力が前記乗算モジュールの第２の入力部に接続されており、前記第２のレジスタ手段が、前記第１、第２、第３の制御信号に応じて前記第１の初期値の乗法逆元を与える、乗法逆元演算回路が提供される。

【００３３】本発明の請求項３の発明によれば、前記第１の初期値と前記第２の初期値とをレジスタ手段へ入力し、前記制御手段は、サイクル数が所定の数ｋ（ｋは、自然数）となった場合に第１のべき乗演算手段にｒ＝２$^{k-1}$、ｓ＝２ｒとしてｓ乗を計算させる第１の制御信号と、第２のべき乗演算手段にｒ＝｛（ｍ－１）ｍｏｄ（２$^{k-1}$）｝＋１、ｓ＝２ｒとしてｓ乗を計算させる第２の制御信号とを入力し、前記乗算モジュールの選択手段には、（ｍ－１）の２進表現でのビットｋ－１が１の場合には前記第２のレジスタ手段の入力に前記第２の乗算手段の出力を入力し、（ｍ－１）の２進表現でのビットｋ－１が１でない場合には前記第２のレジスタ手段の入力に前記第２のレジスタ手段の出力を与える第３の制御信号を入力する、乗法逆元演算回路が提供される。

【００３４】本発明の請求項４の発明によれば、請求項１の乗算モジュール２個と、第１の初期値が設定できる第１のレジスタ手段と、第２の初期値が設定できる第２のレジスタ手段とを含み、前記乗算モジュールのそれぞれ第１の出力を他の前記第１の入力部に接続し、前記乗

算モジュールのそれぞれ第２の出力を他の前記第２の入力部に接続し、前記乗算モジュール群の結合によって得られた回路に対し、前記乗算モジュールの第１の入力部に前記第１のレジスタ手段の出力が接続され、前記乗算モジュールの第２の入力部に前記第２のレジスタ手段の出力が接続され、前記乗算モジュールの第１の出力部に前記第１のレジスタ手段の入力が接続され、前記乗算モジュールの第２の出力部に前記第２のレジスタ手段の入力が接続された乗法逆元演算回路。

【００３５】本発明の請求項５の発明によれば、３個以上の請求項１の乗算モジュールと、第１の初期値が設定できる第１のレジスタ手段と、第２の初期値が設定できる第２のレジスタ手段とを含み、前記乗算モジュールのそれぞれ第１の出力を他の前記第１の入力部に接続し、前記乗算モジュールのそれぞれ第２の出力を他の前記第２の入力部に接続し、前記乗算モジュール群の結合によって得られた回路に対し、前記乗算モジュールの第１の入力部に前記第１のレジスタ手段の出力が接続され、前記乗算モジュールの第２の入力部に前記第２のレジスタ手段の出力が接続され、前記乗算モジュールの第１の出力部に前記第１のレジスタ手段の入力が接続され、前記乗算モジュールの第２の出力部に前記第２のレジスタ手段の入力が接続された乗法逆元演算回路が提供される。

【００３６】本発明の請求項６の発明によれば、前記乗算モジュールの数ｎ（ｎは、自然数）は、$[\log_2(m-1)+1]$以下とされる、乗法逆元演算回路が提供される。

【００３７】本発明の請求項７の発明によれば、制御手段により、ｉ段目（ｎ≧ｉ≧１）の乗算モジュールに対して、サイクル数が所定の数ｑ（ｑは自然数）となった場合に、ｐ＝｛ｎ（ｑ－１）＋ｉ｝として、第１のべき乗演算手段に$r=2^{p-1}$、ｓ＝２ｒとしてｓ乗を計算させる第１の制御信号と、第２のべき乗演算手段に$r=\{(m-1)\bmod(2^{p-1})\}+1$、ｓ＝２ｒとしてｓ乗を計算させる第２の制御信号とを入力し、前記ｉ段目の乗算モジュールの選択手段には、（ｍ－１）の２進表現でのビットｐ－１が１の場合には前記ｉ段目の乗算モジュールの第２の出力に前記第２の乗算手段の出力を与え、（ｍ－１）の２進表現でのビットｐ－１が１でない場合には前記ｉ段目のモジュールの第２の出力に、前記ｉ段目の乗算モジュールへの第２の入力部からのｍビットデータを与える第３の制御信号を入力する、乗法逆元演算回路が提供される。

【００３８】本発明の請求項８の発明によれば、$[\log_2(m-1)+1]$個の請求項１の乗算モジュールと、それぞれの前記乗算モジュールを制御するための第１の制御信号群と、第２の制御信号群と、第３の制御信号群とを与える制御手段とを含み、前記乗算モジュールのそれぞれ第１の出力が次の前記乗算モジュールの第１の入力部に接続され、前記乗算モジュールのそれぞれ第２の出力が次の前記乗算モジュールの前記第２の入力部に接続されており、前記制御手段は、所定段目ｋ（ｋは、自然数）の乗算モジュールに対して、$r=2^{k-1}$、ｓ＝２ｒとしてｓ乗を計算させる第１の制御信号を第１のべき乗演算手段に与え、$r=\{(m-1)\bmod(2^{k-1})\}+1$、ｓ＝２ｒとしてｓ乗を計算させる第２の制御信号を第２のべき乗演算手段に与え、ｍ－１の２進表現におけるビットｋ－１が１の場合に選択手段の出力として第２の乗算手段の出力を与え、ｍ－１の２進表現におけるビットｋ－１が１ではない場合には選択手段の出力として第２の入力部から入力されるｍビットデータを与える、乗法逆元演算回路が提供される。

【００３９】本発明の請求項９の発明によれば、前記乗算モジュールに接続される対となったレジスタ手段を含む、乗法逆元演算回路が提供される。

【００４０】本発明の請求項１０の発明によれば、ガロア体$GF(2^m)$（$m\geqq 1$）上のｍビットデータを乗算するための第１の入力部と第２の入力部とを含む乗算モジュールの制御方式であって、第１および第２のべき乗演算手段に前記第１の入力部からの第１のｍビットデータを入力する段階と、第１の乗算手段に前記第１のｍビットデータおよび前記第１のべき乗演算手段からの出力を入力する段階と、第２の乗算手段に前記第２の入力部からの第２のｍビットデータおよび前記第２のべき乗演算手段からの出力を入力する段階と、選択手段に前記第２の乗算手段の出力信号および前記第２のｍビットデータを入力する段階と、制御回路から前記第１の乗算手段と、前記第２の乗算手段と、前記選択手段とにそれぞれ制御信号を出力する段階とを含み、前記第１のべき乗演算手段に第１の制御信号を入力し、前記第２のべき乗演算手段に第２の制御信号を入力し、前記選択手段に該選択手段の出力を制御するための第３の制御信号を入力し、前記第１の乗算手段に第１の出力信号を出力させ、前記選択手段に第２の出力信号を出力させる、乗算モジュールの制御方式が提供される。

【００４１】本発明の請求項１１の発明によれば、請求項１の乗算モジュールを与える段階と、第１の初期値が設定でき前記乗算モジュールの第１の出力信号が入力される、第１のレジスタ手段を与える段階と、第２の初期値が設定でき前記乗算モジュールの第２の出力信号が入力される、第２のレジスタ手段を与える段階とを含み、前記第１のレジスタ手段の出力が前記乗算モジュールの第１の入力部に接続され、前記第２のレジスタ手段の出力が前記乗算モジュールの第２の入力部に接続されており、さらに、前記第２のレジスタ手段が、前記第１、第２、第３の制御信号に応じて前記第１の初期値の乗法逆元を与える段階とを含む、乗法逆元演算回路の制御方式が提供される。

【００４２】本発明の請求項１２の発明によれば、前記第１の初期値と前記第２の初期値とを入力する段階と、サイクル数が所定の数ｋ（ｋは、自然数）となった場合

に第１のべき乗演算手段にｒ＝2^{k-1}、ｓ＝２ｒとしてｓ乗を計算させる第１の制御信号と、第２のべき乗演算手段にｒ＝｛（ｍ－１）ｍｏｄ（2^{k-1}）｝＋１、ｓ＝２ｒとしてｓ乗を計算させる第２の制御信号とを入力し、前記乗算モジュールの選択手段には、（ｍ－１）の２進表現でのビットｋ－１が１の場合には前記第２のレジスタ手段の入力に前記第２の乗算手段の出力を入力し、（ｍ－１）の２進表現でのビットｋ－１が１でない場合には前記第２のレジスタ手段の入力に前記第２のレジスタ手段の出力を入力するための第３の制御信号を入力する段階を含む、乗法逆元演算回路の制御方式が提供される。

【００４３】本発明の請求項１３の発明によれば、請求項１の乗算モジュール２個と、第１の初期値が設定できる第１のレジスタ手段と、第２の初期値が設定できる第２のレジスタ手段とを含み、前記乗算モジュールのそれぞれ第１の出力を他の前記第１の入力部に接続し、前記乗算モジュールのそれぞれ第２の出力を他の前記第２の入力部に接続した乗法逆元演算回路の制御方式であって、前記乗算モジュールの第１の出力部に前記第１のレジスタ手段の入力が接続され、前記乗算モジュールの第２の出力部に前記第２のレジスタ手段の入力が接続され、前記乗算モジュール群の結合によって得られた回路に対し、前記乗算モジュールの第１の入力部に前記第１のレジスタ手段の出力を接続する段階と、前記乗算モジュールの第２の入力部に前記第２のレジスタ手段の出力を接続する段階と、を含む、乗法逆元演算回路の制御方式が提供される。

【００４４】本発明の請求項１４の発明によれば、３個以上の請求項１の乗算モジュール２個と、第１の初期値が設定できる第１のレジスタ手段と、第２の初期値が設定できる第２のレジスタ手段とを含み、前記乗算モジュールのそれぞれ第１の出力を他の前記第１の入力部に接続し、前記乗算モジュールのそれぞれ第２の出力を他の前記第２の入力部に接続した乗法逆元演算回路の制御方式であって、前記乗算モジュールの第１の出力部に前記第１のレジスタ手段の入力が接続され、前記乗算モジュールの第２の出力部に前記第２のレジスタ手段の入力が接続され、前記乗算モジュール群の結合によって得られた回路に対し、前記乗算モジュールの第１の入力部に前記第１のレジスタ手段の出力を接続する段階と、前記乗算モジュールの第２の入力部に前記第２のレジスタ手段の出力を接続する段階とを含む、乗法逆元演算回路の制御方式が提供される。

【００４５】本発明の請求項１５の発明によれば、前記乗算モジュールの数ｎ（ｎは、自然数）は、$[\log_2(m-1)+1]$以下とされる、乗法逆元演算回路の制御方式が提供される。

【００４６】本発明の請求項１６の発明によれば、ｉ段目（ｎ≧ｉ≧１）の乗算モジュールに対して、サイクル数が所定の数ｑ（ｑは自然数）となった場合に、ｐ＝｛ｎ（ｑ－１）＋ｉ｝として、第１のべき乗演算手段にｒ＝2^{p-1}、ｓ＝２ｒとしてｓ乗を計算させる第１の制御信号と、第２のべき乗演算手段にｒ＝｛（ｍ－１）ｍｏｄ（2^{p-1}）｝＋１、ｓ＝２ｒとしてｓ乗を計算させる第２の制御信号とを入力し、前記乗算モジュールの選択手段には、（ｍ－１）の２進表現でのビットｐ－１が１の場合には前記ｉ段目の乗算モジュールの第２の出力に前記第２の乗算手段の出力を与え、（ｍ－１）の２進表現でのビットｐ－１が１でない場合には前記ｉ段目の乗算モジュールの第２の出力に、前記ｉ段目の乗算モジュールの第２の入力部からのｍビットデータを与える第３の制御信号を入力する、乗法逆元演算回路の制御方式が提供される。

【００４７】本発明の請求項１７の発明によれば、$[\log_2(m-1)+1]$個の請求項１の乗算モジュールを与える段階と、それぞれの前記乗算モジュールを制御するための第１の制御信号群と、第２の制御信号群と、第３の制御信号群とを与える段階とを含み、前記乗算モジュールのそれぞれ前記第１の出力が次の前記第１の入力部に接続され、前記乗算モジュールのそれぞれ前記第２の出力が次の前記第２の入力部に接続されており、所定段目ｋ（ｋは、自然数）の乗算モジュールに対して、ｒ＝2^{k-1}、ｓ＝２ｒとしてｓ乗を計算させる第１の制御信号を第１のべき乗演算手段に与え、ｒ＝｛（ｍ－１）ｍｏｄ（2^{k-1}）｝＋１、ｓ＝２ｒとしてｓ乗を計算させる第２の制御信号を第２のべき乗演算手段に与え、ｍ－１の２進表現におけるビットｋ－１が１の場合に選択手段の出力として第２の乗算手段の出力を与え、ｍ－１の２進表現におけるビットｋ－１が１ではない場合には選択手段の出力として第２の入力部から入力されるｍビットデータを与える段階を含む、乗法逆元演算回路の制御方式が提供される。

【００４８】本発明の請求項１８の発明によれば、前記乗算モジュールからの出力を対となったレジスタ手段に入力する段階を含む、乗法逆元演算回路の制御方式が提供される。

【００４９】本発明の請求項１９の発明によれば、ガロア体$GF(2^m)$（ｍ≧１）上のｍビットデータを乗算するための第１の入力部と第２の入力部とを含む乗算モジュールを用いる装置であって、該乗算モジュールは、前記第１の入力部からの第１のｍビットデータが入力される第１および第２のべき乗演算手段と、前記第１のｍビットデータおよび前記第１のべき乗演算手段からの出力が入力される第１の乗算手段と、前記第２の入力部からの第２のｍビットデータおよび前記第２のべき乗演算手段からの出力が入力される第２の乗算手段と、前記第２の乗算手段の出力信号および前記第２のｍビットデータが入力される選択手段と、前記第１のべき乗演算手段と、前記第２のべき乗演算手段と、前記選択手段とにそれぞれ制

御信号を出力する制御回路とを含んで構成され、前記第１のべき乗演算手段には第１の制御信号が入力され、前記第２のべき乗乗算手段には第２の制御信号が入力され、前記選択手段には該選択手段の出力を制御するための第３の制御信号が入力され、前記第１の乗算手段が第１の出力信号を出力し、前記選択手段が第２の出力信号を出力する装置が提供される。

【００５０】本発明の請求項２０の発明によれば、請求項１の乗算モジュールと、第１の初期値が設定でき前記乗算モジュールの第１の出力信号が入力される、第１のレジスタ手段と、第２の初期値が設定でき前記乗算モジュールの第２の出力信号が入力される、第２のレジスタ手段とを含み、前記第１のレジスタ手段の出力が前記乗算モジュールの第１の入力部に接続され、前記第２のレジスタ手段の出力が前記乗算モジュールの第２の入力部に接続されており、前記第２のレジスタ手段が、前記第１、第２、第３の制御信号に応じて前記第１の初期値の乗法逆元を与える、乗法逆元演算回路を含む装置が提供される。

【００５１】本発明の請求項２１の発明によれば、前記第１の初期値と前記第２の初期値とを入力し、サイクル数が所定の数ｋ（ｋは、自然数）となった場合に第１のべき乗演算手段にｒ＝2^{k-1}、ｓ＝２ｒとしてｓ乗を計算させる第１の制御信号と、第２のべき乗演算手段にｒ＝｛（ｍ－１）ｍｏｄ（2^{k-1}）｝＋１、ｓ＝２ｒとしてｓ乗を計算させる第２の制御信号とを入力し、前記乗算モジュールの選択手段には、（ｍ－１）の２進表現でのビットｋ－１が１の場合には前記第２のレジスタ手段の入力に前記第２の乗算手段の出力を入力し、（ｍ－１）の２進表現でのビットｋ－１が１でない場合には前記第２のレジスタ手段の入力に前記第２のレジスタ手段の出力を入力するための第３の制御信号を入力する、乗法逆元演算回路を含む装置が提供される。

【００５２】本発明の請求項２２の発明によれば、請求項１の乗算モジュール２個と、第１の初期値が設定できる第１のレジスタ手段と、第２の初期値が設定できる第２のレジスタ手段とを含み、前記乗算モジュールのそれぞれ第１の出力を他の前記第１の入力部に接続し、前記乗算モジュールのそれぞれ第２の出力を他の前記第２の入力部に接続し、前記乗算モジュール群の結合によって得られた回路に対し、その第１の入力部に前記第１のレジスタ手段の出力が接続され、前記乗算モジュールの第２の入力部に前記第２のレジスタ手段の出力が接続され、前記乗算モジュールの第１の出力部に前記第１のレジスタ手段の入力が接続され、前記乗算モジュールの第２の出力部に前記第２のレジスタ手段の入力が接続された乗法逆元演算回路を含む、装置。

【００５３】本発明の請求項２３の発明によれば、３個以上の請求項１の乗算モジュールと、第１の初期値が設定できる第１のレジスタ手段と、第２の初期値が設定できる第２のレジスタ手段とを含み、前記乗算モジュールのそれぞれ第１の出力を他の前記第１の入力部に接続し、前記乗算モジュールのそれぞれ第２の出力を他の前記第２の入力部に接続し、前記乗算モジュール群の結合によって得られた回路に対し、その第１の入力部に前記第１のレジスタ手段の出力が接続され、前記乗算モジュールの第２の入力部に前記第２のレジスタ手段の出力が接続され、前記乗算モジュールの第１の出力部に前記第１のレジスタ手段の入力が接続され、前記乗算モジュールの第２の出力部に前記第２のレジスタ手段の入力が接続された乗法逆元演算回路を含む、装置が提供される。

【００５４】本発明の請求項２４の発明によれば、前記乗算モジュールの数ｎ（ｎは、自然数）は、$[\log_2(m-1)+1]$以下とされる乗法逆元演算回路を含む装置が提供される。

【００５５】本発明の請求項２５の発明によれば、制御手段により、ｉ段目（ｎ≧ｉ≧１）の乗算モジュールに対して、サイクル数が所定の数ｑ（ｑは自然数）となった場合に、ｐ＝｛ｎ（ｑ－１）＋ｉ｝として、第１のべき乗演算手段にｒ＝2^{p-1}、ｓ＝２ｒとしてｓ乗を計算させる第１の制御信号と、第２のべき乗演算手段にｒ＝｛（ｍ－１）ｍｏｄ（2^{p-1}）｝＋１、ｓ＝２ｒとしてｓ乗を計算する第２の制御信号とを入力し、前記ｉ番目の乗算モジュールの選択手段には、（ｍ－１）の２進表現でのビットｐ－１が１の場合には前記ｉ番目の乗算モジュールの第２の出力に前記第２の乗算手段の出力を与え、（ｍ－１）の２進表現でのビットｐ－１が１でない場合には前記ｉ番目の乗算モジュールの第２の出力を、前記ｉ段目の乗算モジュールの第２の入力部からのｍビットデータとする第３の制御信号を入力する乗法逆元演算回路を含む、装置が提供される。

【００５６】本発明の請求項２６の発明によれば、$[\log_2(m-1)+1]$個の請求項１の乗算モジュールと、それぞれの前記乗算モジュールを制御するための第１の制御信号群と、第２の制御信号群と、第３の制御信号群とを与える制御手段とを含み、前記乗算モジュールのそれぞれ第１の出力が他の前記乗算モジュールの第１の入力部に接続され、前記乗算モジュールのそれぞれ第２の出力が他の前記乗算モジュールの第２の入力部に接続されており、前記制御手段は、所定段目ｋ（ｋは、自然数）の乗算モジュールに対して、ｒ＝2^{k-1}、ｓ＝２ｒとしてｓ乗を計算させる第１の制御信号を第１のべき乗演算手段に与え、ｒ＝｛（ｍ－１）ｍｏｄ（2^{k-1}）｝＋１、ｓ＝２ｒとしてｓ乗を計算させる第２の制御信号を第２のべき乗演算手段に与え、ｍ－１の２進表現におけるビットｋ－１が１の場合に選択手段の出力として第２の乗算手段の出力を与え、ｍ－１の２進表現におけるビットｋ－１が１ではない場合には選択手段の出力として前記第２の入力部から入力されるｍビットデータを与える乗法逆元演算回路を含む装置が提供される。

21

【００５７】本発明の請求項２７の発明によれば、前記乗算モジュールに接続される対となったレジスタ手段を含む、乗法逆元演算回路が提供される。

【００５８】本発明の請求項２８の発明によれば、ガロア体GF(2m)（m≧1）上のｍビットデータを乗算するため、第１の入力部からｍビットデータおよびべき乗演算手段からの出力を乗算手段に入力する段階と、第２の入力部からのｍビットデータおよび前記べき乗演算手段からの出力を乗算手段に入力する段階とを含む乗法逆元演算回路の制御方式であって、ｐ＝｛ｎ（ｑ－１）＋ｉ｝として、第１のべき乗演算手段にｒ＝2^{p-1}、ｓ＝２ｒとしてｓ乗を計算させる第１の制御信号と、第２のべき乗演算手段にｒ＝｛（ｍ－１）ｍｏｄ（2^{p-1}）｝＋１、ｓ＝２ｒとしてｓ乗を計算する第２の制御信号とを入力する段階と、ｍ－１の２進表現におけるビットｋ－１（ｋは、自然数）が１の場合に選択手段の出力として第２の乗算手段の出力を与え、ｍ－１の２進表現におけるビットｋ－１が１ではない場合には選択手段の出力として前記第２の入力部から入力されるｍビットデータを与える段階とを含む、乗法逆元演算回路の制御方式が提供される。

【００５９】本発明の請求項２９の発明によれば、ガロア体GF(2m)（m≧1）上のｍビットデータを乗算するため、第１の入力部からｍビットデータおよびべき乗演算手段からの出力を乗算手段に入力する段階と、第２の入力部からのｍビットデータおよび前記べき乗演算手段からの出力を乗算手段に入力する段階とを含む乗算方法を実行させるためのソースコードが記録されたコンピュータ可読な記録媒体であって、該記録媒体は、ｐ＝｛ｎ（ｑ－１）＋ｉ｝として、第１のべき乗演算手段にｒ＝2^{p-1}、ｓ＝２ｒとしてｓ乗を計算させる第１の制御信号と、第２のべき乗演算手段にｒ＝｛（ｍ－１）ｍｏｄ（2^{p-1}）｝＋１、ｓ＝２ｒとしてｓ乗を計算する第２の制御信号とを入力し、ｍ－１の２進表現におけるビットｋ－１（ｋは、自然数）が１の場合に選択手段の出力として第２の乗算手段の出力を与え、ｍ－１の２進表現におけるビットｋ－１が１ではない場合には選択手段の出力として前記第２の入力部から入力されるｍビットデータを与える、記録媒体が提供される。

【００６０】本発明の請求項３０の発明によれば、ガロア体GF(2m)（m≧1）上のｍビットデータを乗算するため、第１の入力部からｍビットデータおよびべき乗演算手段からの出力を乗算手段に入力する段階と、第２の入力部からのｍビットデータおよび前記べき乗演算手段からの出力を乗算手段に入力する段階とを含む乗算方法を実行させるためのソースコードが記録されたコンピュータ可読な伝送媒体であって、該伝送媒体は、ｐ＝｛ｎ（ｑ－１）＋ｉ｝として、第１のべき乗演算手段にｒ＝2^{p-1}、ｓ＝２ｒとしてｓ乗を計算させる第１の制御信号と、第２のべき乗演算手段にｒ＝｛（ｍ－１）ｍｏｄ

22

（2^{p-1}）｝＋１、ｓ＝２ｒとしてｓ乗を計算する第２の制御信号とを入力し、ｍ－１の２進表現におけるビットｋ－１（ｋは、自然数）が１の場合に選択手段の出力として第２の乗算手段の出力を与え、ｍ－１の２進表現におけるビットｋ－１が１ではない場合には選択手段の出力として前記第２の入力部から入力されるｍビットデータを与える、伝送媒体が提供される。

【００６１】本発明の請求項３１の発明によれば、ガロア体GF(2m)（m≧1）上のｍビットデータを乗算するため、第１の入力部からのｍビットデータおよびべき乗演算手段からの出力が入力される乗算手段と、第２の入力部からのｍビットデータおよび前記べき乗演算手段からの出力が入力される乗算手段とを含む暗号装置であって、ｐ＝｛ｎ（ｑ－１）＋ｉ｝として、第１のべき乗演算手段にｒ＝2^{p-1}、ｓ＝２ｒとしてｓ乗を計算させる第１の制御信号と、第２のべき乗演算手段にｒ＝｛（ｍ－１）ｍｏｄ（2^{p-1}）｝＋１、ｓ＝２ｒとしてｓ乗を計算させる第２の制御信号とを入力するための手段と、ｍ－１の２進表現におけるビットｋ－１（ｋは、自然数）が１の場合に選択手段の出力として第２の乗算手段の出力を与え、ｍ－１の２進表現におけるビットｋ－１が１ではない場合には選択手段の出力として前記第２の入力部から入力されるｍビットデータを与えるための手段と、を含む暗号装置が提供される。

【００６２】本発明の請求項３２の発明によれば、ガロア体GF(2m)（m≧1）上のｍビットデータを乗算するため、第１の入力部からのｍビットデータおよびべき乗演算手段からの出力が入力される乗算手段と、第２の入力部からのｍビットデータおよび前記べき乗演算手段からの出力が入力される乗算手段とを含む誤り訂正復号器であって、ｐ＝｛ｎ（ｑ－１）＋ｉ｝として、第１のべき乗演算手段にｒ＝2^{p-1}、ｓ＝２ｒとしてｓ乗を計算させる第１の制御信号と、第２のべき乗演算手段にｒ＝｛（ｍ－１）ｍｏｄ（2^{p-1}）｝＋１、ｓ＝２ｒとしてｓ乗を計算する第２の制御信号とを入力するための手段と、ｍ－１の２進表現におけるビットｋ－１（ｋは、自然数）が１の場合に選択手段の出力として第２の乗算手段の出力を与え、ｍ－１の２進表現におけるビットｋ－１が１ではない場合には選択手段の出力として前記第２の入力部から入力されるｍビットデータを与えるための手段と、を含む誤り訂正復号器が提供される。

【００６３】本発明の請求項３３の発明によれば、ガロア体GF(2m)（m≧1）上のｍビットデータを乗算するため、第１の入力部からのｍビットデータおよびべき乗演算手段からの出力が入力される乗算手段と、第２の入力部からのｍビットデータおよび前記べき乗演算手段からの出力が入力される乗算手段とを含む装置であって、ｐ＝｛ｎ（ｑ－１）＋ｉ｝として、第１のべき乗演算手段にｒ＝2^{p-1}、ｓ＝２ｒとしてｓ乗を計算させる第１の制御信号と、第２のべき乗演算手段にｒ＝｛（ｍ－１）

ｍｏｄ（2^{p-1}）｝＋１、ｓ＝２ｒとしてｓ乗を計算する第２の制御信号とを入力するための手段と、ｍ－１の２進表現におけるビットｋ－１（ｋは、自然数）が１の場合に選択手段の出力として第２の乗算手段の出力を与え、ｍ－１の２進表現におけるビットｋ－１が１ではない場合には選択手段の出力として前記第２の入力部から入力されるｍビットデータを与えるための手段と、を含む装置が提供される。

【００６４】

【発明の実施の形態】以下、本発明の図面に示した実施例をもって説明する。本発明においては、Ｈｗ（χ）はχの２進表現におけるハミング重み、［χ］はχの整数部（小数部を切り捨てた数）、ａは、GF(2ᵐ)の原始多項式の根、ａ０は、GF(2ᵐ)における１、Ｍは乗算回路のレイテンシを表わすものとする。また、レジスタＲ１およびＲ２（これらについては後述）へ値を設定してから、次に値を設定するまでの期間を、１サイクルとする。

【００６５】図４の乗算モジュール（基本演算モジュール）を用い、順序回路として乗法逆元演算回路を構成する場合は図５または図６のように、組み合わせ回路として実現する場合は図７のように回路を構成する。図５ないし図７における基本モジュール等の制御信号は、図８のように与える。図６における制御信号については後述する。また、後述する図１２のようにパイプライン化することもできる。

【００６６】ここで、基本的な乗算モジュールは、２個の乗算回路と２個の２のべき乗演算回路（２ᵏ乗演算を行う）、および出力Ｂのセレクタで構成される。各べき乗演算回路においてｋをいくつにとるかは、モジュールの制御信号として外部より与えられる（図４）。順序回路として実現する場合（図５、図６）、図４の乗算モジュールを１個以上用い、その出力をレジスタに接続する。レジスタは初期値が設定できるものを用い、その初期値は外部より与えられる。レジスタ出力は乗算モジュール群の入力へフィードバックされる。乗算モジュールやセレクタの制御は、専用の制御手段、例えばコントロール回路によって行う。そのコントロール回路は、図８の手順に従って各制御信号を生成する。

【００６７】図８のアルゴリズムを回路として実装する実施例について説明する。このアルゴリズムから得られるデータフローグラフを、回路実装に用いる。各部品を組み合わせ回路で構成したうえでデータフローグラフ全体を静的に回路展開すれば組み合わせ回路が得られるし，リソースアロケーションとスケジューリングを行って順序回路とすることもできる。順序回路とする場合，乗算やべき乗演算などは必ずしもパラレル入出力である必要はない。

【００６８】なお，上記アルゴリズムでは

【００６９】

【数１０】

$$(m-1)\ \mathrm{mod}\ (2^{k-1})$$

などと剰余演算を行っているように見える個所があるが，これは実際には「ｍ－１の２進表現のうち下位ｋ－１ビットを抽出する」操作で，きわめて軽いハードで実現できる（組み合わせ回路にする場合は，これらは定数値となるので，事前計算による回路簡単化が可能）。また、２のべき乗演算も簡単な回路で作れるので基本的に乗算とレジスタだけのコストと考えてよい。

【００７０】さて、このアルゴリズムを順序回路化したとき，ｍが動的に変化できるようにするのは簡単である。レジスタはｍによらずＲ１とＲ２の２つであり、それらの役割がｍによって変わることはない。ｍに依存して変化するのは、ループの回数と、べき乗演算のべき数だけであり、データパスの構造はｍにほとんど依存しない。データパスをコントロールするために、ｍからべき数

【００７１】

【数１１】

$$\{(m-1)\ \mathrm{mod}\ (2^{k-1})+1\}$$

の動的導出をしなければならないが、それはきわめて容易で、上記のとおりｍ－１の２進表現からビットを切り出すだけで行える。

【００７２】組み合わせ回路として実現する場合（図７）、図４の基本構成モジュールを直列に、

【００７３】

【数１２】

$$[\log_2(m-1)]+1$$

個接続する。各モジュールの制御信号は、図８の手順に従って与えられる。その制御信号はｍを固定すれば固定値となるので、それにより論理を簡単化できる。なお、ｍを別のレジスタで持っておき、そこから制御信号をデコードすることにより、任意のｍに対処できるような回路を構成してもよい。

【００７４】図５の変形として、乗算モジュールを下記式

【００７５】

【数１３】

$$[\log_2(m-1)+1] \geqq n \geqq 1$$

の範囲内のｎ個を直列に接続して得られる回路に、図５と同様にレジスタと各モジュールの制御回路を付加して回路を構成することもできる（図６）。そのｑ（ｑは、自然数）サイクル目において、ｉ段目（ｎ≧ｉ≧１）のモジュールの制御入力には、図８のｎ（ｑ－１）＋ｉサイクル目の制御信号を与える。たとえば、３段直列に接続した場合、１段目のモジュールには図８の１，４，７，…サイクル目の制御信号、２段目のモジュールには２，

５，８，…サイクル目の制御信号、３段目のモジュールには３，６，９，…サイクル目の制御信号を、サイクルごとに与える。

【００７６】なお、本発明は、図４、図５、図６、図７、図１２から冗長論理を削除して得られる回路をすべて含む。とくに、一方の入力に常に定数ａ０が与えられる乗算回路は削除し、他方の入力をその出力と直結する。また、出力が使われないべき乗演算回路や、出力が固定の選択回路も削除する。さらに、図４において、乗算回路やべき乗演算回路などは必ずしも組み合わせ回路である必要はない。

【００７７】ｍ＝１５の組み合わせ回路を例に、実際にどのような制御信号をモジュールに与えるかを図９に示す。

【００７８】ｍ＝１５の場合、基本モジュールを４つ直列につなげた構造となる。モジュール番号を、入力側から１，２，３，４とする。このとき、図９に示すようにたとえばモジュール２には次のような制御信号を与える。

○べき乗演算回路１は、４乗演算を行う。
○べき乗演算回路２は、２乗演算を行う。
○選択回路は、出力Ｂに入力Ｂの値を出す。

他のモジュールについても同様である。ここで、モジュール１，２の乗算回路２、モジュール４の乗算回路１、モジュール１のべき乗演算回路２、モジュール４のべき乗演算回路１は、いずれも不要となるので削除し、それによって得られた回路を用いる。

【００７９】ｍ＝１５で、図５のような順序回路として実現する場合、レジスタを初期化した後、４サイクルかけて処理を行う。基本回路モジュールへの制御信号は、

Ｆｅｒｍａｔ：｛[$\log_2(m-2)$]+1｝＊乗算器のレイテンシ
伊東　　：｛[$\log_2(m-1)$]+Hw(m-1)-1｝＊乗算器のレイテンシ
本手法　　：[$\log_2(m-2)$]+1｝＊乗算器のレイテンシ

で、Ｆｅｒｍａｔと本手法がもっとも良い。伊東のアルゴリズムと本手法のレイテンシの違いを、図１０のグラフに示す.

【００８３】以上をまとめると、本手法は、回路サイズを伊東と同じでＦｅｒｍａｔよりはるかに少なく保ったまま、伊東の約半分の（＝Ｆｅｒｍａｔと同じ）レイテンシに改善できる。また、図６下段のとおり、実際に汎用論理合成ツールで実回路を作成した場合にも、上記アルゴリズムの差がそのままゲート数や速度に現れる。図１１には、本発明において、ｍ＝１４、１５、１６とした場合のデータフローグラフを示す。

【００８４】図１２には、本発明の乗法逆元演算回路のさらに別の実施例を示す。図１２の乗法逆元演算回路は、図７に示した実施例の構成に加えて、レジスタＲ１，Ｒ２が追加されている。これらの対となったレジスタＲ１，Ｒ２は、図１２に示した乗法逆元演算回路を構成する乗算モジュールのいかなる位置においても、また

＊図９におけるモジュール１，２，３，４と同じものをこの順に与える。制御信号の生成は、図５におけるべき乗レジスタ入力制御信号生成回路で行う。

【００８０】他のｍについても、同様に基本モジュールの接続と制御を行う。

（１）図５のように順序回路として実装した場合：計算にかかるサイクル数は、任意のｍに対し、

Ｆｅｒｍａｔ：　ｍ－２
伊東　　：　[$\log_2(m-1)$]+Hw(m-1)-1
本発明　　：　[$\log_2(m-1)$]+1

で、本発明がもっとも良く、最大で伊東の約半分で計算できる。

たとえばｍ＝１９２の場合

Ｆｅｒｍａｔ：　１９０
伊東　　：　１３
本発明　　：　８

また、ｍ＝５１１の場合、

Ｆｅｒｍａｔ：　５０９
伊東　　：　１５
本手法　　：　９

となり、大きくレイテンシが改善される。

【００８１】（２）図７のように組み合わせ回路として実装した場合：乗算回路の個数（回路サイズ）は、任意のｍに対し、

Ｆｅｒｍａｔ：　ｍ－２
伊東　　：　[$\log_2(m-1)$]+Hw(m-1)-1
本発明　　：　[$\log_2(m-1)$]+Hw(m-1)-1

で、伊東と本手法がもっとも良い.

【００８２】また、レイテンシ（スピード）は、いかなる個数でも配置することができる。

【００８５】

【発明の効果】上述したように、本発明によれば、基本モジュールを組み合わせた形で、低いレイテンシ（順序回路の場合は少ない処理クロック数、組み合わせ回路の場合は少ディレイ）を乗算回数を増やすことなく達成することができる。

【００８６】本手法では、動的にｍを変えるのが、Ｆｅｒｍａｔと同程度に容易である（順序回路として実装した場合）。レジスタの個数が２個と静的に決まっているので、任意のｍでほぼ同じデータパスが使え、ループ回数などのコントロールを変更するだけでｍを変更できる。コントロールを動的に変更するのも先述のとおり簡単な回路でできる。本手法は、逆元演算のみならず、べき乗演算の高速化に応用できる。

【００８７】本手法は、文献[4]等にあるComposite Fieldベースの高速化手法と組み合わせることで、より一層

27

の回路規模縮小／レイテンシ短縮を実現できる。これまで本発明の図面に示した実施例をもって説明してきたが、本発明は図面に示した実施例に限定されるものではなく、種々の変更、除外、別の態様が可能である。また、本発明を適用することができる装置は、暗号装置、誤り復号装置ばかりではなく、ガロワ拡大体を用いるいかなる装置に対しても適用できることは言うまでもないことである。

【図面の簡単な説明】

【図１】Fermatの定理を用いた従来の乗法逆元演算のアルゴリズムを示した図。

【図２】従来の乗法逆元演算のアルゴリズムを木構造を用いて示した図。

【図３】従来の乗法逆元演算のアルゴリズムを示した図。

【図４】本発明の乗法モジュールを示した図。

【図５】本発明の乗法逆元演算回路を示した図。

【図６】本発明の乗法逆元演算回路の別の実施例を示した図。

【図７】本発明の乗法逆元演算回路のさらに別の実施例を示した図。

28

*【図８】本発明に用いる制御信号を与えるため擬似コードを示した図。

【図９】本発明に用いる制御信号を例示した図。

【図１０】本アルゴリズムと従来のアルゴリズムとのレイテンシを比較した図。

【図１１】本発明のアルゴリズムによるデータフローグラフとスケジューリングを示した図。

【図１２】図７に示した乗法逆元演算回路にレジスタを含ませたさらに別の実施例を示した図。

【符号の説明】

ｕ１…第１のべき乗演算手段
ｕ２…第２のべき乗演算手段
ｕ３…第１の乗算手段
ｕ４…第２の乗算手段
ｕ５…選択手段
Ｓ０…第３の制御信号
Ｓ１…第１の制御信号
Ｓ２…第２の制御信号
Ｒ１…第１のレジスタ手段
Ｒ２…第２のレジスタ手段

【図１】

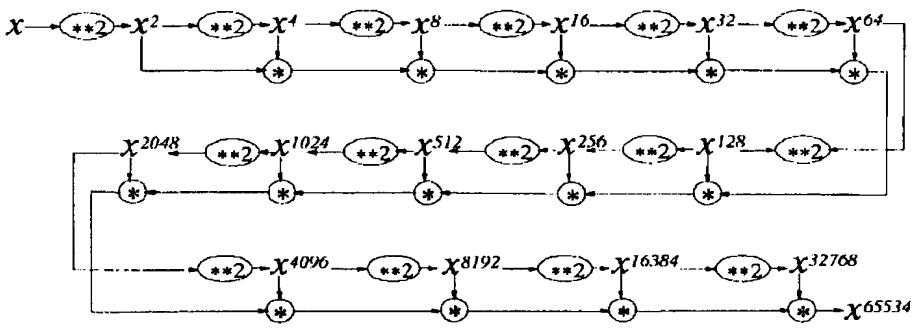


図1　Fermatの定理による計算過程の例(m=16)

【図４】

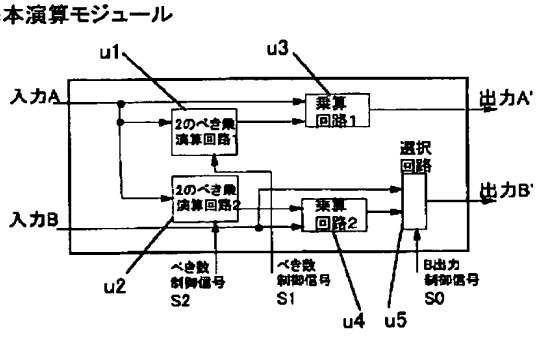
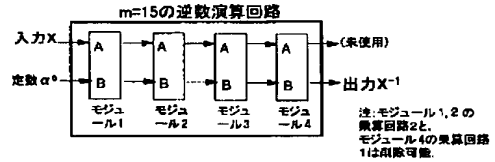


図4　回路の構成に用いる乗算デバイス

【図９】



	べき数制御S1	べき数制御S2	出力B制御S0
モジュール１	2^1乗	(べき乗不要)	入力B
モジュール２	2^2乗	2^1乗	入力B
モジュール３	2^4乗	2^3乗	乗算回路2出力
モジュール４	(べき乗不要)	2^7乗	乗算回路2出力

図9　各モジュールへ与える制御信号の具体例(m=15)

【図２】

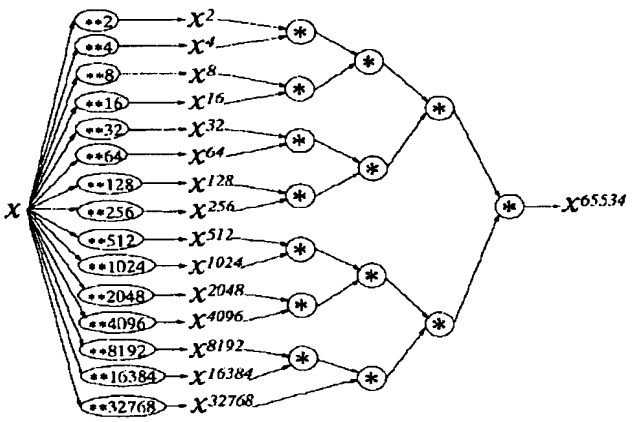


図2　　Fermatの定理による計算過程の例(m=16)

【図３】

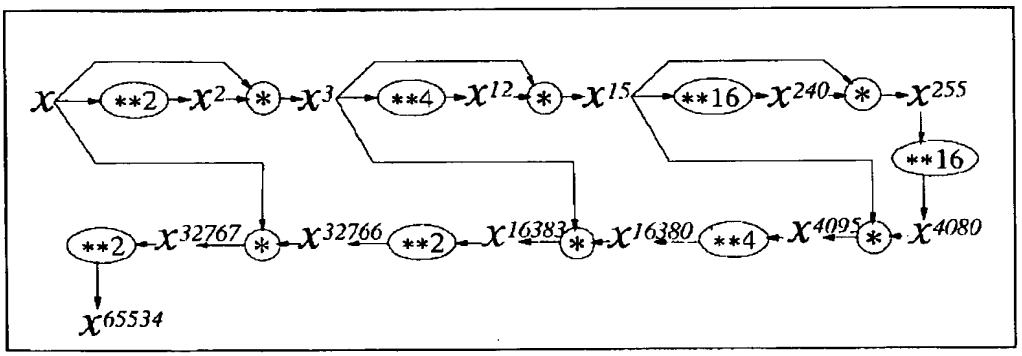


図3　　伊東・辻井のアルゴリズムによる計算過程の例(m=16)

【図８】

1．順序機械として実現する場合：

以下を$\lfloor \log_2(m-1) \rfloor$ 回繰り返す

kサイクル目において,(kは0始まり)

べき乗演算回路1は，2^{2^k}乗を計算

べき乗演算回路2は，$2^{\{(m-1) \bmod (2^{k+1})\}}+1$乗乗を計算

レジスタR1の入力に乗算回路1の出力を選択

$m-1$の2進表現においてビット$k-1$が1なら

レジスタR2の入力に乗算回路2の出力を選択

そうでなければ

レジスタR2の入力にレジスタ2の出力を選択

2．組み合わせ回路として実現する場合：

入力側から出力側へ向かって順にモジュール 1, 2, 3, …として，モジュールkの制御信号は

べき乗演算回路1は，$2^{2^{k-1}}$乗を計算

べき乗演算回路2は，$2^{\{(m-1) \bmod (2^{k+1})\}}+1$乗乗を計算

$m-1$の2進表現においてビット$k-1$が1なら

出力Bに乗算回路2の出力を選択

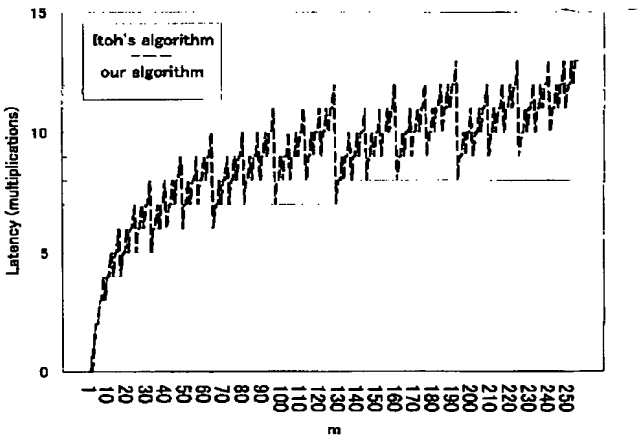
そうでなければ

出力Bに入力Bを選択

なお，組み合わせ回路として実現する場合，一方の入力に常に定数α^0が与えられる乗算回路は削除し，他方の入力をその出力と直結する．

図8　　各モジュールの制御信号の具体的な生成法

【図１０】



【図５】

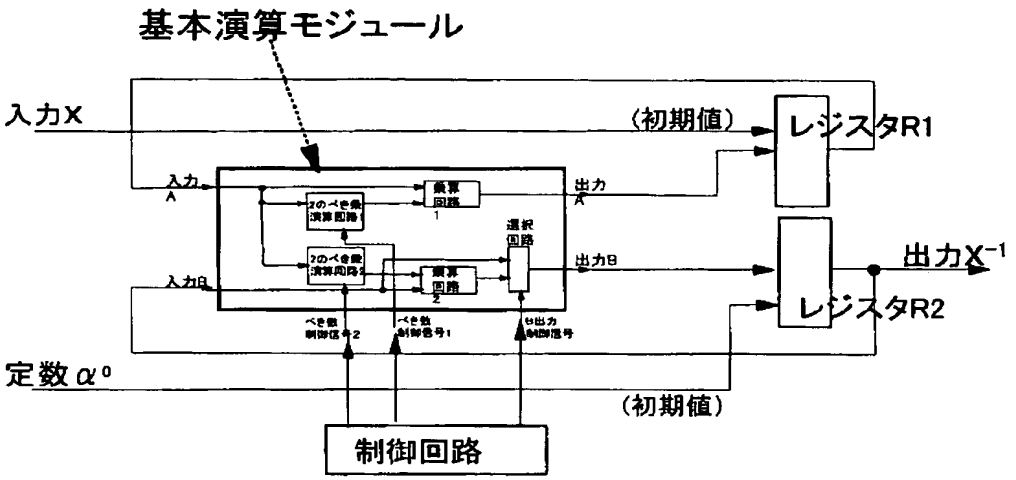


図5　順序機械として実現する場合の全体構成法1

【図６】

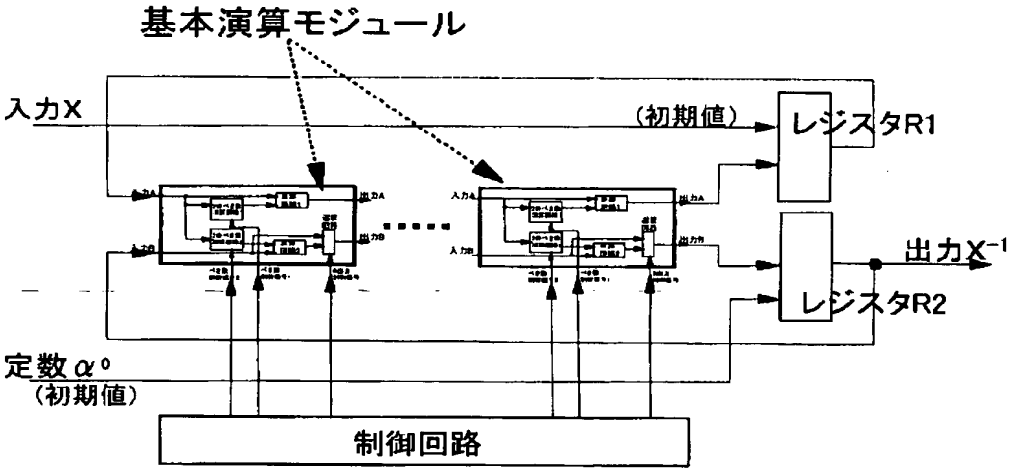


図6　順序回路として実現する場合の全体構成法2

【図７】

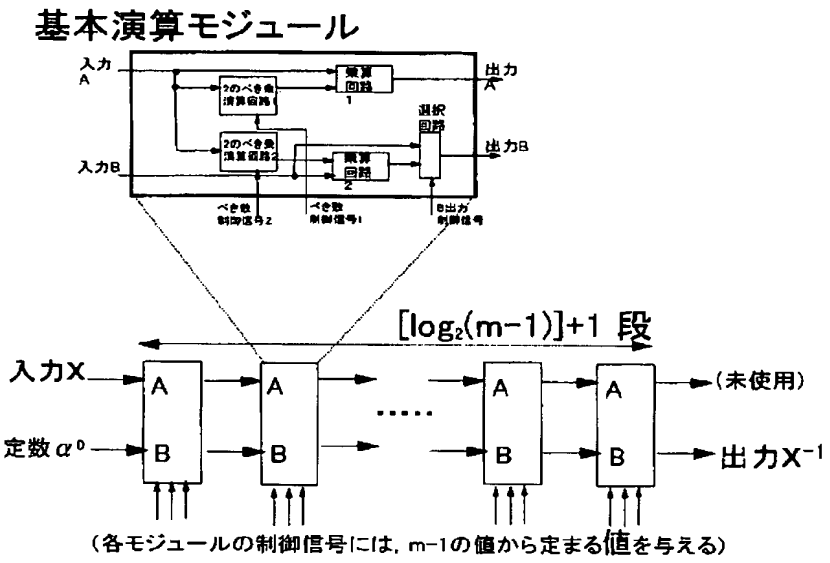
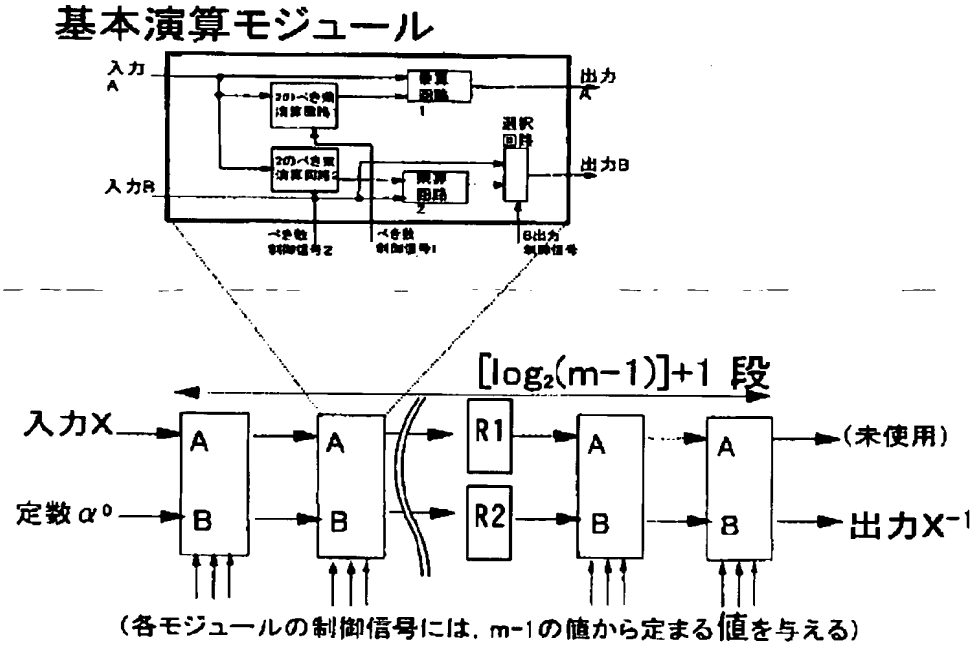
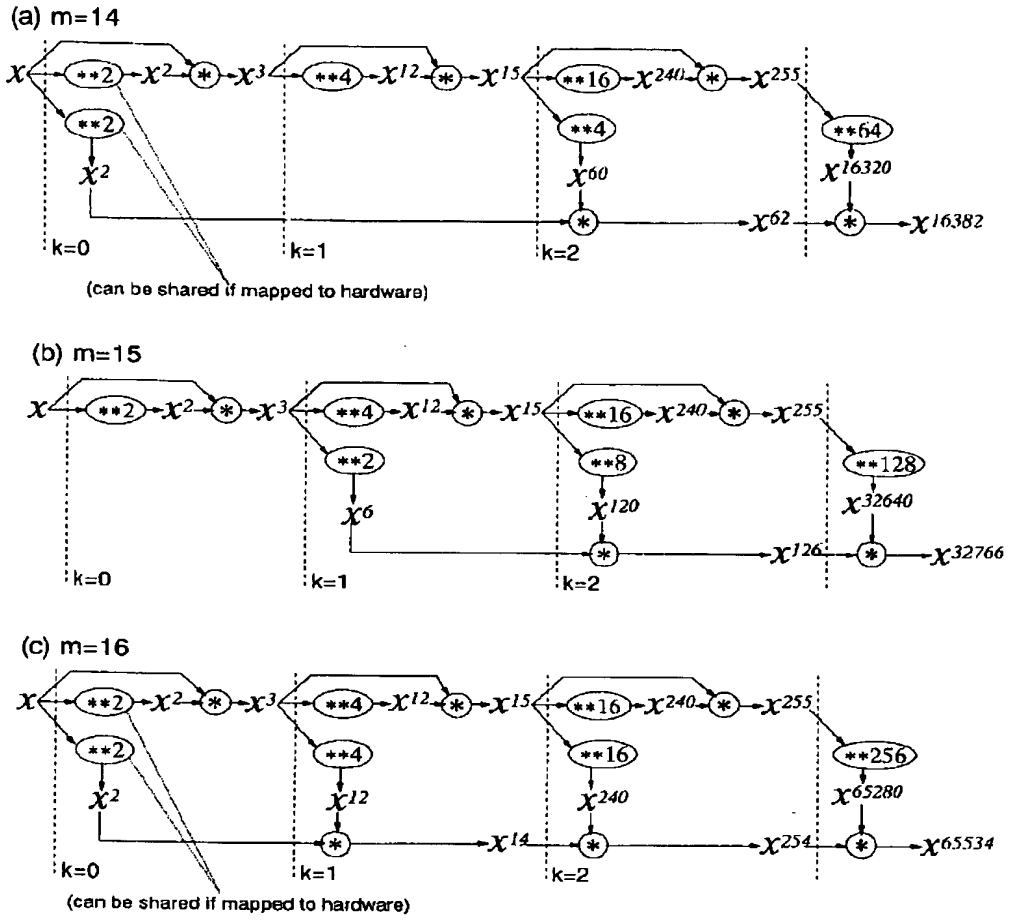


図7　　組み合わせ回路として実現する場合の全体構成法

【図１２】



【図１１】



【手続補正書】
【提出日】平成１３年５月１日（２００１．５．１）
【手続補正１】
【補正対象書類名】図面
【補正対象項目名】図５
【補正方法】変更
【補正内容】
【図５】

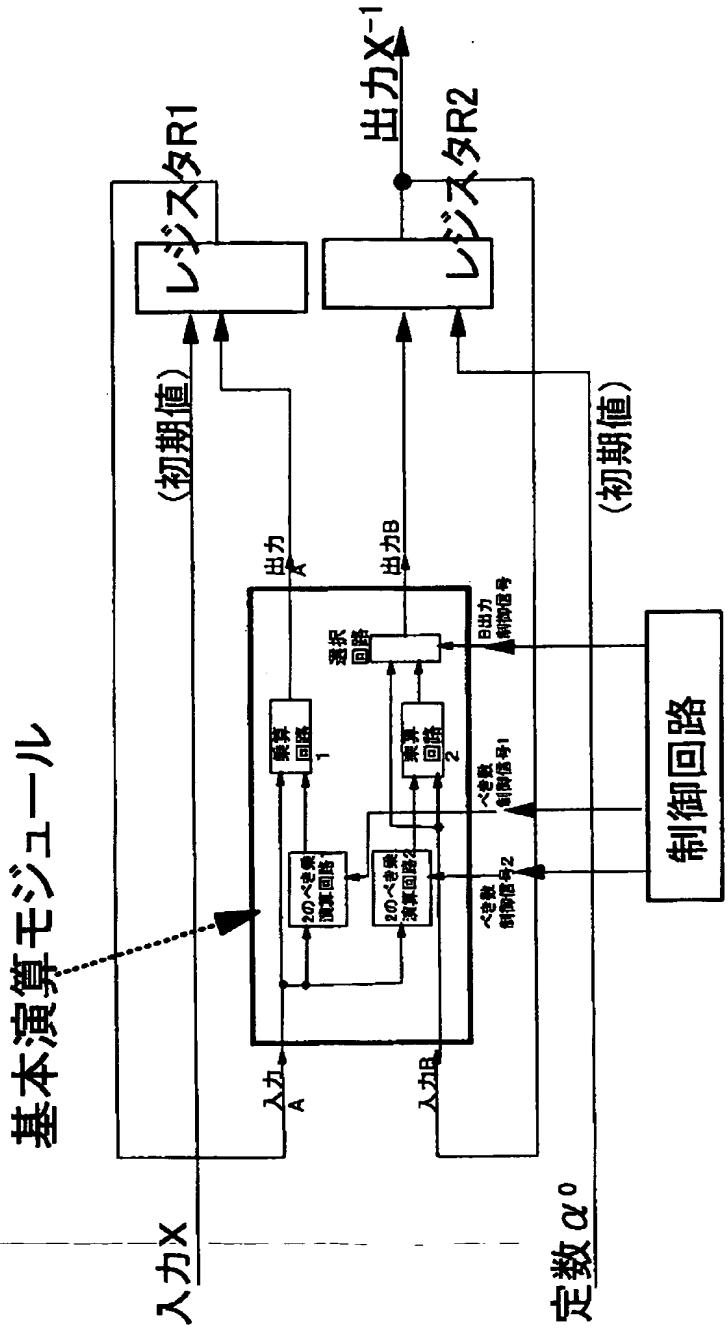


図5　順序機械として実現する場合の全体構成法1

【手続補正２】
【補正対象書類名】図面
【補正対象項目名】図６

【補正方法】変更
【補正内容】
【図６】

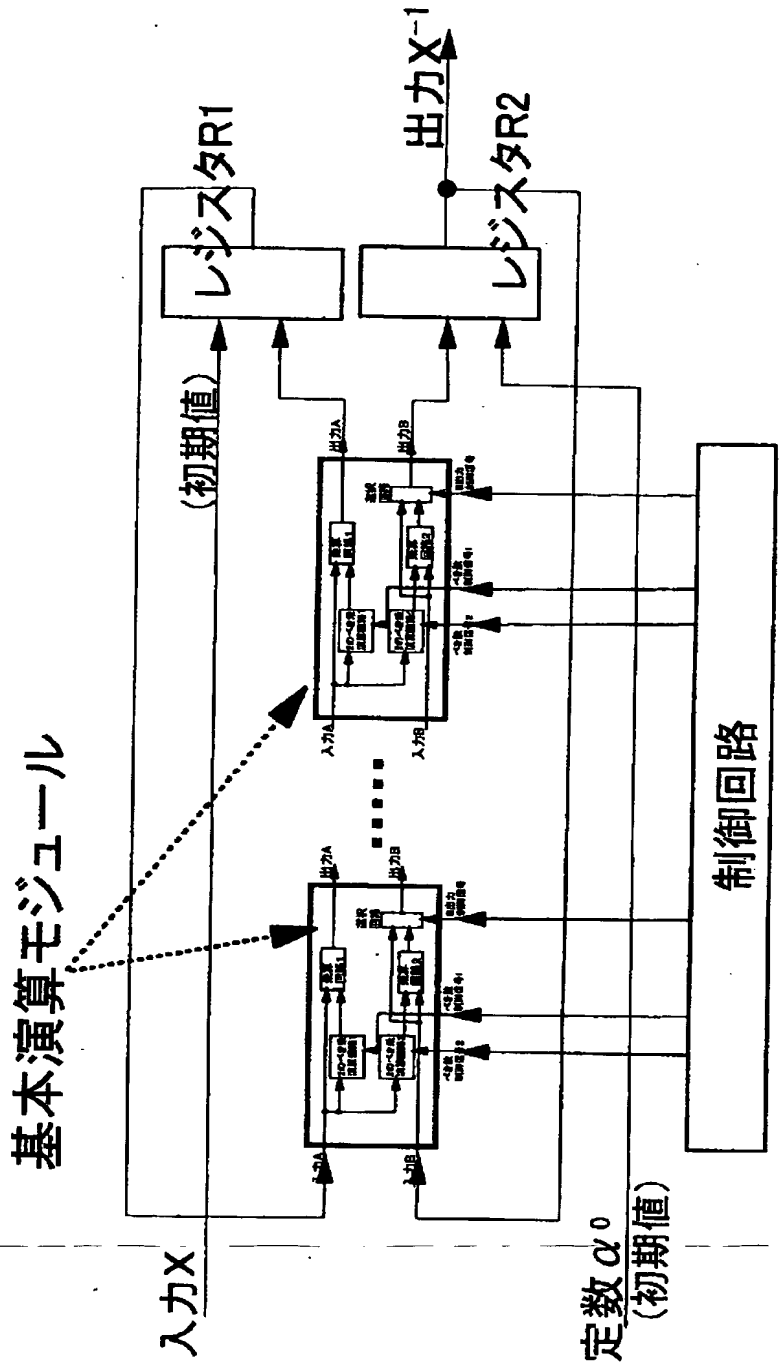


図6　順序回路として実現する場合の全体構成法2

【手続補正３】
【補正対象書類名】図面
【補正対象項目名】図７

【補正方法】変更
【補正内容】
【図７】

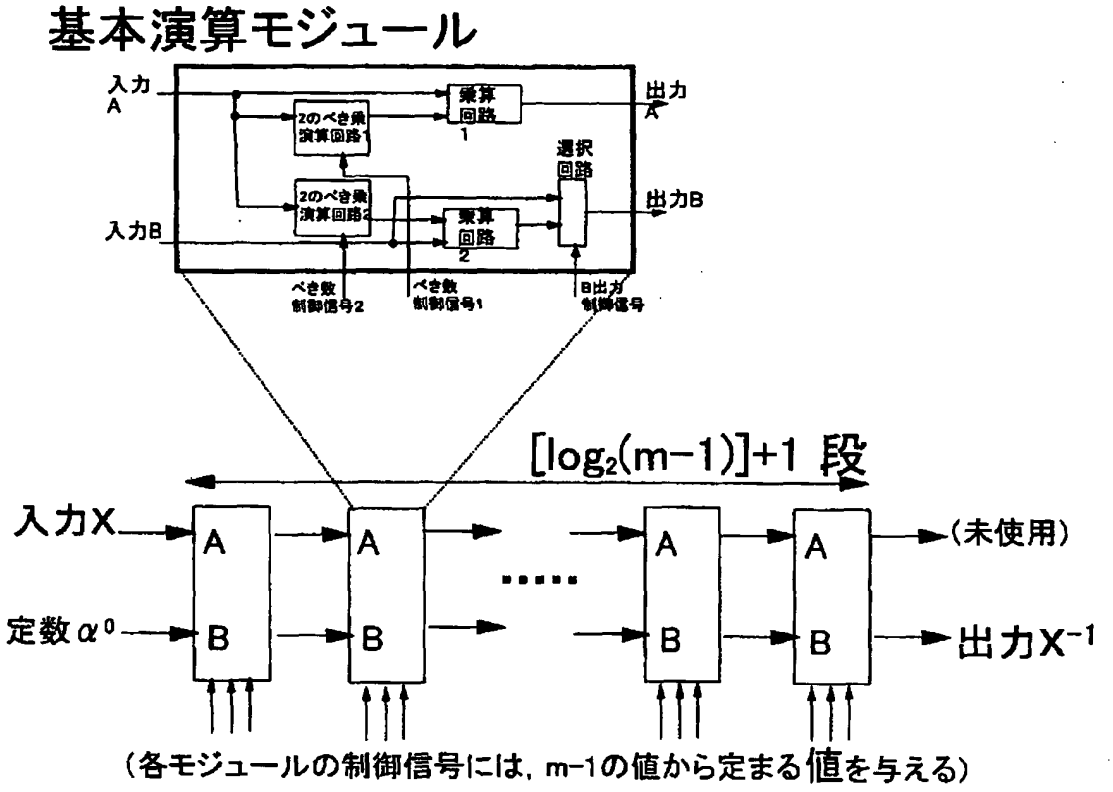


図7　　組み合わせ回路として実現する場合の全体構成法

フロントページの続き

(72) 発明者　森岡　澄夫
神奈川県大和市下鶴間1623番地14　日本アイ・ビー・エム株式会社　東京基礎研究所内

(72) 発明者　片山　泰尚
神奈川県大和市下鶴間1623番地14　日本アイ・ビー・エム株式会社　東京基礎研究所内

Fターム(参考)　5J104 AA22 NA18